카스퍼스키 안티 바이러스 2010

사용자 가이드

프로그램 버전: 9.0 CRITICAL FIX 2

KASPERSKY lab

카스퍼스키 안티 바이러스 2010 사용 고객님께!

카스퍼스키 랩 제품을 선택해 주셔서 감사합니다.

이 문서가 고객님의 제품 사용에 대한 답변을 제공할 수 있을 것입니다.

번역물을 포함한 다양한 유형의 복제 및 배포는 카스퍼스키 랩의 사전 허가를 얻어야만 합니다.

이 문서와 그래픽 이미지는 정보성, 비상업적 및 개인 용도로서만 사용할 수 있습니다.

이 문서는 사전 공지 없이 수정될 수 있습니다. 이 문서의 최신 버전은 카스퍼스키랩 웹사이트 http://www.kaspersky.co.kr 을 참조하십시오.

카스퍼스키랩은 문서의 내용, 품질, 관련성, 정확성에 대해 보증하지 않으며 문서 사용에 따른 잠정적인 피해에 대해 어떠한 책임도 지지 않습니다.

이 문서는 등록 및 비등록 상표를 포함합니다. 모든 등록 상표는 그 소유자의 재산입니다.

© 1997-2009 Kaspersky Lab ZAO. All Rights Reserved

http://www.kaspersky.com
http://www.kaspersky.co.kr

목차

소개 11

배포 도구 11

정품 사용자를 위한 서비스 제공 12

하드웨어와 소프트웨어 시스템 요구사항 12

카스퍼스키 안티 바이러스 2010 13

프로그램 정보 보기 13

직접 참조 가능한 정보 출처 13

영업 부서에 문의 14

기술 지원 서비스에 문의 14

고객 포럼에서 카스퍼스키 랩 프로그램에 대해 토론 15

카스퍼스키 안티 바이러스 2010 의 새로운 기능 16

컴퓨터 감시 개념 17

실시간 감시 구성요소 17

바이러스 검사 작업 19

업데이트 20

데이터 및 온라인 활동 실시간 감시 20

마법사 및 도구 20

프로그램의 지원 기능 21

카스퍼스키 안티 바이러스 설치 23

1 단계. 새 버전의 프로그램 검색 24

2 단계. 설치 조건에 시스템이 부합하는지 확인 24

3 단계. 설치 유형 선택 24

4 단계. 최종 사용자 동의서 25

5 단계. 카스퍼스키 시큐리티 네트워크 데이터 수집 성명 25

6 단계. 설치 폴더 선택 25

7 단계. 설치할 프로그램 구성요소 선택 25

8 단계. 이전 설치 시에 저장된 프로그램 설정 사용 26

9 단계. 다른 안티 바이러스 프로그램 검색 26

10 단계. 설치 최종 준비 27

11 단계. 설치 완료 27

시작하기 28

프로그램 구성 마법사 29

1 단계. 프로그램 활성화 29
2 단계. 감시 모드 선택 31
3 단계. 프로그램 업데이트 구성 31
4 단계. 프로그램 접근 차단 32
5 단계. 탐지할 보안위협 선택 32
6 단계. 마법사 종료 33
프로그램 업데이트 33
컴퓨터 바이러스 검사 33
컴퓨터 취약점 검사 34
라이센스 관리 34
자동 라이센스 갱신 신청 35
카스퍼스키 시큐리티 네트워크 참가 36
보안 관리 37
실시간 감시 상태 39
실시간 감시 일시 중지 40
프로그램 인터페이스 41
알림 영역 아이콘 41
마우스 오른쪽 메뉴 42
카스퍼스키 안티 바이러스 메인 창 43
알림 46
프로그램 설정 창 46
컴퓨터 파일 시스템 실시간 감시 47
구성요소 연산 알고리즘 48
파일 및 메모리의 보안 레벨 변경 49
탐지된 개체에 수행할 처리 방법 변경 50
감시 영역 생성 50
휴리스틱 분석 사용 51
검사 최적화 52
복합 파일 검사 52
대용량 복합 파일 검사 53
감시 방식 변경 54
고급 감시 기술 54
구성요소 일시 중지: 스케줄 생성 55
구성요소 일시 중지: 프로그램 목록 생성 56
기본 감시 설정 복원 57

메일 실시간 감시 58
구성요소 연산 알고리즘 59
이메일 실시간 감시 보안 레벨 변경 60
탐지된 개체에 수행할 처리 방법 변경 61
실시간 감시 영역 생성 62
MICROSOFT OFFICE OUTLOOK 의 이메일 검사 62
THE BAT!의 이메일 검사 63
휴리스틱 분석기 사용 64
복합 파일 검사 64
첨부파일 필터링 64
기본 메일 감시 설정 복원 65
웹 트래픽 실시간 감시 66
구성요소 연산 알고리즘 67
HTTP 트래픽 보안 레벨 변경 68
탐지된 개체에 수행할 처리 방법 변경 68
실시간 감시 영역 생성 69
검사 형태 선택 69
카스퍼스키 URL 분석기 70
휴리스틱 분석 사용 72
감시 최적화 72
기본 웹 감시 설정 복원 73
인스턴트 메신저 트래픽 감시 74
구성요소 연산 알고리즘 75
실시간 감시 영역 생성 75
감시 방법 선택 75
휴리스틱 분석기 사용 76
사전 방역 77
위험 활동 목록 사용 77
위험 활동 감시 규칙 변경 78
신뢰하는 프로그램 그룹 생성 79
시스템 계정 제어 79
컴퓨터 검사 81
바이러스 검사 81
바이러스 검사 작업 시작 83

작업 실행 바로가기 생성 84
검사할 개체 목록 생성 84
보안 레벨 변경 85
탐지된 개체에 수행할 처리 방법 변경 86
검사할 개체 형태 변경 86
검사 최적화 87
이동식 디스크 드라이브 검사 88
복합 파일 검사 88
고급 감시 기술 89
검사 방법 변경 90
스케줄: 스케줄 생성 90
스케줄: 계정 지정 91
스케줄된 작업 실행 기능 91
기본 검사 설정 복원 92
취약점 검사 92
취약점 검사 작업 시작 93
작업 실행 바로가기 생성 94
검사할 개체 목록 생성 94
스케줄: 스케줄 생성 95
스케줄: 계정 지정 95
업데이트 96
업데이트 시작 97
마지막으로 성공한 업데이트로 롤백 98
업데이트 경로 선택 98
프록시 서버 사용 99
지역 설정 100
업데이트 후 수행할 처리 방법 100
로컬 폴더에서 업데이트 101
업데이트 작업 스케줄 변경 101
다른 사용자 계정으로 업데이트 실행 102
프로그램 설정 구성 103
실시간 감시 104
실시간 감시 작동/중지 105
시스템 시작 시 카스퍼스키 안티 바이러스 실행 105
대화식 실시간 감시 모드 사용 106

카스퍼스키 안티 바이러스 접근 제한 106
파일 안티 바이러스 107
메일 안티 바이러스 108
웹 안티 바이러스 108
메신저 안티 바이러스 109
사전 방역 110
검사 110
업데이트 111
설정 112
카스퍼스키 안티 바이러스 자기-보호 기능 112
고급 치료 기술 113
랩탑에서 카스퍼스키 안티 바이러스 사용 113
작업 실행 중의 컴퓨터 성능 114
카스퍼스키 안티 바이러스 설정 내보내기/가져오기 114
기본 설정 복원 115
탐지할 보안위협 및 제외 115
네트워크 120
알림 124
리포트 및 저장소 126
정보 제공 129
프로그램 인터페이스 130
카스퍼스키 안티 바이러스 프로필 사용 131
추가 기능 133
보안 키보드 133
응급 복구 디스크 134
응급 복구 디스크 제작 135
응급 복구 디스크를 사용하여 컴퓨터 부팅 136
브라우저 구성 137
감염 후 복원 138
개인정보보호 마법사 138
리포트 140
리포트를 생성할 구성요소 또는 작업 선택 141
리포트에서 정보 그룹 표시 관리 141
리포트 준비 알림 142
이벤트 유형 선택 142

화면에 데이터 표시 143
통계 정보에 대한 표 또는 그래픽 표시 144
파일로 리포트 저장 145
복잡한 필터링 사용 145
이벤트 검색 146
알림 148
악성 개체 탐지 149
개체 치료 불가 150
고급 치료 기술 필요 151
트래픽에서 위험 개체 탐지 151
감염의심 개체 탐지 151
시스템에서 위험 활동 탐지 152
숨겨진 프로세스 탐지 153
시스템 레지스트리 접근 시도 탐지 154
피싱 공격 탐지 154
감염의심 링크 탐지 155
잘못된 인증서 탐지 155
카스퍼스키 안티 바이러스 설정 확인 156
테스트 "바이러스" EICAR 및 변종 156
HTTP 트래픽 감시 테스트 158
SMTP 트래픽 감시 테스트 158
파일 안티 바이러스 설정 확인 159
바이러스 검사 작업 설정 확인 159
명령줄을 통한 프로그램 작업 160
프로그램 활성화 162
프로그램 구성요소 및 작업 관리 162
바이러스 검사 164
프로그램 업데이트 168
마지막으로 성공한 업데이트로 롤백 169
감시 설정 내보내기 169
감시 설정 가져오기 170
프로그램 시작 170
프로그램 중지 170
추적 파일 생성 170
도움말 보기 171

명령줄 반환 코드 171
문제 제거 173
시스템 상태 리포트 생성 173
추적 파일 생성 174
데이터 파일 전송 175
AVZ 스크립트 실행 176
카스퍼스키 시큐리티 네트워크 데이터 수집 정책 177
타사 코드 사용 181
CRYPTO C LIBRARY (데이터 시큐리티 소프트웨어 라이브러리) ..... **오류! 책갈피가 정의되어 있지 않습니다.**
FASTSCRIPT 1.9 라이브러리 182
LIBNKFM 7.4.7.7 라이브러리 182
GNU 분석 라이브러리 183
AGG 2.4 라이브러리 183
OPENSSL 0.9.8D 라이브러리 184
GECKO SDK 1.8 라이브러리 185
ZLIB 1.2 라이브러리 186
LIBPNG 1.2.8, 1.2.29 라이브러리 186
LIBNKFM 2.0.5 라이브러리 186
EXPAT 1.2, 2.0.1 라이브러리 186
INFO-ZIP 5.51 라이브러리 186
WINDOWS INSTALLER XML (WIX) 2.0 LIBRARY 187
PASSTHRU 라이브러리 191
FILTER 라이브러리 191
NETCFG 라이브러리 191
PCRE 3.0 라이브러리 191
RFC1321-BASED (RSA-FREE) MD5 라이브러리 191
WINDOWS TEMPLATE 라이브러리 (WTL 7.5) 191
LIBJPEG 6B 라이브러리 195
LIBUNGIF 3.0 라이브러리 196
LIBXDR 라이브러리 197
TINICONV - 1.0.0 라이브러리 197
BZIP2/LIBBZIP2 1.0.5 라이브러리 204
LIBSPF2-1.2.9 라이브러리 204
PROTOCOL BUFFER 라이브러리 205

용어집 206

카스퍼스키 랩 216

카스퍼스키 랩 최종 사용자 라이센스 계약 217

소개

참조:

배포 도구 11

정품 사용자를 위한 서비스 제공 12

하드웨어와 소프트웨어 시스템 요구사항 12

배포 도구

오프라인 유통사에서 카스퍼스키 안티 바이러스의 패키지 버전을 구매하거나, http://www.kaspersky.co.kr 의 온라인 쇼핑몰에서 인터넷 시큐리티를 구매할 수 있습니다.

프로그램의 패키지 버전을 구매하면 아래와 같은 항목으로 구성됩니다.:

- 봉인 된 패키지에 프로그램 파일과 PDF 형식의 설명서가 들어있는 설치 CD.
- 퀵 매뉴얼 문서.
- 활성화 코드 및 홈페이지 고객등록번호

최종 사용자 사용권 계약은 소비자와 카스퍼스키 랩 사이의 소비자가 구입한 소프트웨어를 사용할 수 있는 기간을 명시한 법적인 협정입니다.

홈페이지 등의 최종 사용자 사용권 계약을 신중하게 읽어주세요!

만약 최종 사용자 사용권 계약에 동의를 하지 않는다면 아직 개봉하지 않은 패키지를 제공함으로써 여러분이 구매한 유통사에 반품이 가능하고, 프로그램을 구매한 가격을 환불 받을 수 있습니다.

봉인된 설치 패키지를 개봉하면 최종 사용자 사용권 계약의 모든 조건에 동의한 것 입니다.

설치 디스크 패키지를 개봉하기 전에 신중하게 최종 사용자 사용권 계약을 읽으시기 바랍니다.

만약, 온라인 쇼핑몰에서 카스퍼스키 안티 바이러스를 구매했다면, 카스퍼스키 랩 웹사이트에서 제품을 다운받을 수 있으며, 사용자 가이드는 설치 패키지에 포함되어있습니다. 결재가 완료 되면 이메일로 활성화 코드를 받게될 것입니다.

정품 사용자를 위한 서비스 제공

카스퍼스키랩은 법적으로 등록된 사용자들이 프로그램을 안정적으로 사용하도록 다양한 서비스를 제공합니다.

라이센스를 구매하고 나면, 정식 사용자로 등록되고 라이센스 기간동안 다음과 같은 서비스를 제공받을 수 있습니다. (단, 홈페이지에 고객등록를 해야 합니다.)

- 매시간 프로그램 데이터베이스 업데이트와 최신 소프트웨어 패키지제공
- 설치 관련 이슈와 구매한 소프트웨어 제품 사용과 설정, 기타 제품 이슈에 대한 지원. 서비스는 전화 또는 이메일을 통하여 제공
- 전세계에 나타난 새로운 바이러스와 새로운 카스퍼스키랩 제품에 대한 알림. 이 서비스는 기술지원 서비스 웹 사이트의 카스퍼스키랩 뉴스 메일링에 등록한 사용자에게 제공됩니다. (http://support.kaspersky.com/subscribe).

사용 중 운영체제 사용과 실행에 관련된 문제, 또는 카스퍼스키 기술 이외의 사항에 대하여 지원하지 않습니다.

하드웨어와 소프트웨어 시스템 요구사항

프로그램의 기능을 정상적으로 사용하려면 다음 최소 요구사항을 충족시켜야 합니다.

일반 요구사항:

- 300 MB 이상의 하드디스크 여유공간.
- CD-ROM (설치 CD 를 사용해서 프로그램 설치 시).
- Microsoft Internet Explorer 6.0 나 그 이상(인터넷으로 프로그램 데이터베이스와 모듈 업데이트를 위해).
- Microsoft Windows Installer 2.0.

- *Microsoft Windows XP Home Edition (Service Pack 2),* Microsoft Windows XP Professional (Service Pack 2), Microsoft Windows XP Professional x64 Edition*:*
  - Intel Pentium 300 MHz 프로세서 또는 그 이상 (또는 동급의 호환 CPU).
  - 256 MB RAM.
- *Microsoft Windows Vista Home Basic, Microsoft Windows Vista Home Premium, Microsoft Windows Vista Business, Microsoft Windows Vista Enterprise, Microsoft Windows Vista Ultimate:*
  - Intel Pentium 800 MHz 32-bit (x86) / 64-bit (x64) 프로세서 또는 그 이상 (또는 동급의 호환 CPU).
  - 512 MB RAM.
- *Microsoft Windows 7 Home Premium, Microsoft Windows 7 Professional, Microsoft Windows 7 Ultimate:*
  - Intel Pentium 1 GHz 32-bit (x86) / 64-bit (x64) 프로세서 또는 그 이상 (또는 동급의 호환 CPU).
  - 1 GB RAM (32-bit); 2 GB RAM (64-bit).

카스퍼스키 안티 바이러스 2010

카스퍼스키 안티 바이러스 2010 은 새로운 차원의 정보 감시 솔루션을 제공합니다.

다른 카스퍼스키 랩 제품을 포함한 다른 소프트웨어와 구별되는 카스퍼스키 안티 바이러스 2010 의 가장 큰 특징은 다양한 접근 방식으로 데이터를 보호할 수 있는 것입니다.

참조:

프로그램 정보 보기 13

프로그램 정보 보기

카스퍼스키 안티 바이러스의 구매, 설치 또는 사용에 대해 질문이 있는 경우 쉽게 답변을 받을 수 있습니다.

카스퍼스키 랩에서는 프로그램에 대한 정보를 다양한 방식으로 제공합니다. 질문의 긴급한 정도와 중요도에 따라 가장 적합한 방법을 선택할 수 있습니다.

참조:

직접 참조 가능한 정보 출처 13

영업 부서에 문의 14

기술 지원 서비스에 문의 14

고객 포럼에서 카스퍼스키 랩 프로그램에 대해 토론 15

직접 참조 가능한 정보 출처

프로그램에 대한 정보를 참조할 수 있는 곳은 다음과 같습니다.:

- 카스퍼스키 랩 웹사이트의 프로그램 페이지;
- 기술 지원 서비스 웹사이트의 FAQ(자주 묻는 질문) 게시판;
- 도움말 시스템;
- 사용 설명서.

카스퍼스키 랩 웹사이트의 프로그램 페이지

http://www.kaspersky.co.kr/homeuser_kav.html

이 페이지에서는 프로그램의 기능 및 옵션과 같은 일반적인 정보를 제공합니다.

기술 지원 서비스 웹사이트의 FAQ(자주 묻는 질문) 게시판

http://www.kaspersky.co.kr/productlink/faqboard.html

이 게시판에는 기술 지원 서비스 전문가가 작성한 문서가 나와 있습니다.

이런 문서에는 프로그램의 구매, 설치 및 사용과 관련된 유용한 정보, 권장 사항 등의 FAQ 가 포함되어 있습니다.

도움말 시스템

프로그램 설치 패키지에는 컴퓨터 감시를 관리하는 방법(감시 상태 보기, 여러 컴퓨터 바이러스 검사, 기타 작업 실행)에 대한 정보, 적절한 설정 목록 및 설명, 실행할 작업 목록과 같은 각 프로그램에 대한 정보가 들어 있는 전체 및 컨텍스트 도움말이 포함되어 있습니다.

도움말 파일을 열려면 도움말이 필요한 창에서 **도움말** 버튼을 누르거나 **<F1>** 키를 누릅니다.

사용 설명서

카스퍼스키 안티 바이러스 설치 패키지에는 PDF 형식의 사용 설명서가 들어 있습니다. 이 설명서에서는 메인 작업 알고리즘과 프로그램의 기능 및 옵션에 대해 설명합니다.

영업 부서에 문의

카스퍼스키 안티 바이러스를 선택 또는 구입하거나 라이센스를 연장하는 데 대한 질문이 있는 경우 다음 전화 번호로 연락하여 영업 부서에 문의하시기 바랍니다.:

(02) 508-8773,

또는 영업 부서로 이메일(sales@kaspersky.co.kr)을 보낼 수도 있습니다.

기술 지원 서비스에 문의

카스퍼스키 안티 바이러스를 이미 구매했다면 전화 또는 인터넷을 통해 기술 지원 서비스에서 카스퍼스키 안티 바이러스에 대한 정보를 얻을 수 있습니다.

기술 지원 서비스 전문가가 카스퍼스키 안티 바이러스를 설치 및 사용과 관련된 질문에 대답해 드립니다. 또한 컴퓨터가 감염되었을 때 악성 프로그램 활동으로 인한 결과를 제거할 수 있도록 도움을 줍니다.

기술 지원 서비스에 연락하기 전에 아래 지원 규칙을 읽어 주십시오.

기술 지원 서비스에 대한 이메일 요청

기술 지원 서비스는 사용자의 질문에 대해 이메일로 답장에 드립니다.

이메일 문의 시 상세한 내용 및 연락 가능한 전화 번호, 고객등록번호, 구입한 제품 명 등을 같이 적어 주시기 바랍니다.

전화 기술 지원

㈜한국카스퍼스키랩 기술 지원 서비스에 전화로 문의할 수 있습니다.

전화 번호: 02-508-8789

전화 지원 시간: 평일(월 ~ 금) - 09:00 ~ 18:00

주말 및 공유일은 이메일 및 고객 포럼을 통해 문의해 주시기 바랍니다

고객 포럼에서 카스퍼스키 랩 프로그램에 대해 토론

질문에 대한 대답을 빨리 받지 않아도 된다면 카스퍼스키 랩 전문가 또는 http://www.kaspersky.co.kr/forum_login.html 의 다른 포럼 사용자와 해당 질문에 대해 토론할 수 있습니다.

이 포럼에서는 기존 항목을 보고, 의견을 남기고, 새 항목을 만들고 검색 엔진을 사용할 수 있습니다.

카스퍼스키 안티 바이러스 2010 의 새로운 기능

카스퍼스키 안티 바이러스 2010 은 포괄적인 데이터 감시 도구입니다. 모든 데이터 전송 및 교환 채널에 대한 다양한 감시 기능을 제공하며 모든 구성요소를 유연하게 구성할 수 있어 사용자는 자신의 구체적인 요구 사항에 맞게 카스퍼스키 안티 바이러스를 변경할 수 있습니다.

이제 카스퍼스키 안티 바이러스 2010 의 혁신적인 새 기능에 대해 자세히 살펴보겠습니다.

새 감시 기능:

- 새 구성요소인 메신저 안티 바이러스는 다양한 인스턴트 메시징 프로그램의 작업 보안을 관리합니다. 이 구성요소는 악성 개체가 있는 메시지를 검사합니다.
- 카스퍼스키 안티 바이러스에는 웹 안티 바이러스로 관리되는 URL 검사 모듈이 포함되어 있습니다. 웹 페이지의 링크가 의심스러운 웹 주소 및 피싱 웹 주소 목록에 포함되는지를 확인하는 이 모듈은 Microsoft Internet Explorer 및 Mozilla Firefox 브라우저에 플러그인으로 내장되어 있습니다.
- 메시지와 웹 페이지의 링크를 검사하고 웹사이트에 접근하려는 시도가 탐지될 때 피싱 주소의 데이터베이스를 사용하여 피싱 웹사이트 접근 감시 및 피싱 공격에 대한 감시를 수행합니다. 웹 주소가 피싱 웹 주소 목록에 포함되어 있는지 검사할 수 있습니다. 이 옵션은 웹 안티 바이러스, 메신저 안티 바이러스에 대해서만 사용할 수 있습니다.
- 취약점 검사라고 하는 새 도구가 검사 작업 목록에 추가되었습니다. 이 도구는 컴퓨터에 설치된 프로그램 및 운영 체제 설정의 보안위협 및 취약점을 쉽게 탐지하고 제거합니다.

새 인터페이스 기능:

- 실시간 감시라고 하는 새로운 감시 관리 방법이 구현되었습니다. 컴퓨터 감시는 사용자 파일 및 개인 데이터, 운영 체제 개체 및 컴퓨터에 설치된 프로그램, 네트워크 활동 등 3 가지 영역에 대해 수행됩니다. 카스퍼스키 안티 바이러스의 특정 구성요소는 이와 같은 각 감시 대상에 적용됩니다. 실시간 감시를 사용하여 사용자는 특정 리소스 카테고리를 감시하고 자신의 설정 편집으로 신속하게 전환하는 구성요소를 알 수 있습니다.
- 컴퓨터에 대한 보안을 제공하는 특정 작업을 실행할 수 있는 마법사 및 도구는 **보안 서비스+**에 그룹화되어 있습니다.

컴퓨터 감시 개념

카스퍼스키 안티 바이러스는 알려지거나 알려지지 않은 보안위협, 네트워크 및 침입자 공격, 스팸 및 기타 원하지 않는 데이터에 대해 사용자의 컴퓨터를 보호합니다. 각각의 보안위협은 별도의 프로그램 구성요소에서 처리합니다. 이런 감시 시스템 구조로 이 프로그램은 회사의 특정 요구 또는 전체 요구에 맞게 유연하게 구성될 수 있습니다.

카스퍼스키 안티 바이러스는 다음과 같은 감시 도구로 구성되어 있습니다:

- 대상 구성요소. 감시 대상:
  - 파일 및 개인 데이터;
  - 시스템;
  - 네트워크 활동.
- 바이러스 검사 작업. 개별 파일, 폴더, 드라이브, 영역 또는 전체 컴퓨터에서 바이러스를 검사하는 데 사용됨.
- 업데이트. 악성 프로그램 검사, 네트워크 공격 및 스팸 메시지 탐지에 사용되는 데이터베이스 및 내부 프로그램 모듈을 최신 상태로 유지.
- 마법사 및 도구. 카스퍼스키 안티 바이러스 작동 중에 발생하는 작업을 편리하게 수행할 수 있도록 도움을 줌.
- 지원 기능. 프로그램으로 작업 및 기능 확장을 지원하는 정보 제공.

참조:

대상 구성요소 17

바이러스 검사 작업 19

업데이트 20

데이터 및 온라인 활동 감시 20

마법사 및 도구 20

프로그램의 지원 기능 21

실시간 감시 구성요소

컴퓨터를 실시간으로 보호해 주는 실시간 감시 구성요소는 다음과 같습니다.

파일 안티 바이러스

파일 안티 바이러스는 컴퓨터의 파일 시스템을 감시합니다. 컴퓨터에서 열거나 실행하거나 저장하는 모든 파일 및 연결된 모든 디스크 드라이브를 검사합니다. 카스퍼스키 안티 바이러스는 모든 파일 접근 시도를 가로채서 파일에 알려진 바이러스가 있는지 검사합니다. 파일은 감염되지 않았거나 카스퍼스키 안티 바이러스에서 성공적으로 처리된 경우에만 계속 사용할 수 있습니다. 어떠한 이유로 파일을 치료할 수 없는 경우 파일이 삭제되며 파일 복사본이 백업 저장소에 저장되거나 격리저장소로 이동됩니다.

메일 안티 바이러스

메일 안티 바이러스는 컴퓨터에서 전송 및 수신되는 모든 이메일 메시지를 검사합니다. 이메일에 악성 프로그램이 있는지 분석합니다. 이메일은 악성 개체가 포함되지 않은 경우에만 수취인이 열어볼 수 있습니다. 또한 메일 안티 바이러스는 이메일 메시지를 분석하여 피싱을 탐지합니다.

웹 안티 바이러스

웹 안티 바이러스는 웹사이트에서 보안위협이 되는 스크립트를 가로채어 차단합니다. 모든 HTTP 트래픽이 철저하게 감시됩니다. 또한 웹 안티 바이러스는 웹페이지를 분석하여 피싱을 탐지합니다.

메신저 안티 바이러스

메신저 안티 바이러스는 메신저를 안전하게 사용할 수 있도록 해 줍니다. IM 프로토콜을 통해 컴퓨터에 전송된 정보를 감시하며 다양한 메신저 프로그램이 안전하게 작동되도록 보호합니다.

사전방역

사전 방역은 신종 악성 프로그램이 악성 활동을 수행하기 전에 이를 탐지합니다. 컴퓨터에 설치된 모든 프로그램의 행동을 감시하고 분석합니다. 카스퍼스키 안티 바이러스는 프로그램이 수행한 행동에 따라 잠재적인 위험성 여부를 판단합니다. 이 프로그램이 위험할 가능성이 있다면? 알려진 바이러스뿐만 아니라 아직 발견되지 않은 신종 바이러스로부터 컴퓨터를 보호할 수 있습니다.

안티 피싱

안티 피싱은 웹 안티 바이러스와 메신저 안티 바이러스에 통합되어 있으며 웹사이트가 피싱 및 의심스러운 웹사이트 목록에 포함되어 있는지 확인합니다.

다음과 같은 실시간 감시 구성요소는 카스퍼스키 인터넷 시큐리티 2010 에서만 사용가능합니다.

프로그램 제어

프로그램 제어는 시스템에 설치된 프로그램에서 수행하는 활동을 기록하고 할당한 그룹을 기반으로 프로그램을 관리합니다. 각 프로그램 그룹에는 특정 규칙이 정의되며 이러한 규칙에 따라 프로그램의 리소스 접근이 관리됩니다.

방화벽

방화벽은 로컬 네트워크 또는 인터넷에서 사용자 작업의 보안을 유지합니다. 이 구성요소는 프로그램 규칙 및 패킷 규칙을 사용하여 모든 네트워크 활동을 필터링합니다.

사전 방역

사전 방역은 신종 악성 프로그램이 악성 활동을 수행하기 전에 이를 탐지합니다. 컴퓨터에 설치된 모든 프로그램의 행동을 감시하고 분석합니다. 카스퍼스키 안티 바이러스는 프로그램이 수행한 행동에 따라 잠재적인 위험성 여부를 판단합니다. 따라서 알려진 바이러스뿐만 아니라 아직 발견되지 않은 신종 바이러스로부터 컴퓨터를 보호할 수 있습니다.

네트워크 공격 차단

네트워크 공격 차단은 운영 체제 시작 시 로딩되며 들어오는 네트워크 트래픽에서 네트워크 공격에 특징적인 활동이 있는지 추적합니다. 컴퓨터 공격 시도가 탐지될 경우 카스퍼스키 안티 바이러스는 컴퓨터를 공격하는 모든 네트워크 활동을 차단합니다.

안티 스팸

안티 스팸은 컴퓨터에 설치된 메일 클라이언트에 통합되어 수신되는 모든 이메일 메시지의 스팸 여부를 감시합니다. 스팸이 포함된 모든 메시지는 특별한 헤더로 표시됩니다. 스팸 처리(자동 삭제, 특별 폴더로 이동 등)에 대한 구성 옵션도 제공됩니다. 또한 안티 스팸은 이메일 메시지를 분석하여 피싱을 탐지합니다.

네트워크 모니터

네트워크 활동에 대한 정보를 실시간으로 표시합니다.

안티 배너

안티 배너는 컴퓨터에 설치된 다양한 프로그램 인터페이스에 내장되어 있거나 웹사이트에 표시되는 배너 광고 정보를 차단합니다.

유해 사이트 차단

유해 사이트 차단 구성요소는 사용자의 웹사이트 접근을 감시합니다. 주요 목적은 포르노, 무기, 마약, 잔인한 행위, 폭력 등을 다루는 성인 전용 웹사이트 또는 시간(채팅룸, 게임) 또는 금전(온라인 스토어, 경매)을 낭비할 수 있는 웹사이트에 대한 접근을 차단하는 것입니다.

바이러스 검사 작업

악성 프로그램이 침투하지 못하도록 방지하는 방법 이외에 컴퓨터에서 바이러스 검사를 정기적으로 수행하는 것이 매우 중요합니다. 정기적인 검사는 보안 레벨이 낮게 설정되었거나 다른 이유로 보안 구성요소가 발견하지 못한 악성 프로그램이 확산되지 않도록 하는 데 필요합니다.

카스퍼스키 안티 바이러스에서는 다음과 같은 바이러스 검사 기능을 제공합니다.:

- **개체 검사**. 사용자가 선택한 개체를 검사합니다. 컴퓨터의 파일 시스템에 있는 어떠한 개체도 검사할 수 있습니다.
- **전체 검사**. 전체 컴퓨터를 완전히 검사합니다. 기본적으로 시스템 메모리, 시작 시 로딩된 프로그램, 시스템 백업, 이메일 데이터베이스, 하드 드라이브, 이동식 저장 장치, 네트워크 드라이브 등은 검사 대상입니다.

- **빠른 검사**. 운영 체제 시작 개체에 바이러스가 있는지 검사합니다.

업데이트

네트워크 공격을 차단하고, 바이러스 또는 기타 악성 프로그램을 삭제하려면 카스퍼스키 안티 바이러스를 정기적으로 업데이트해야 합니다. **업데이트** 구성요소는 이러한 용도로 디자인되었으며 프로그램에 사용되는 프로그램 데이터베이스와 모듈을 업데이트합니다.

업데이트 배포 서비스를 사용하면 카스퍼스키 랩 서버에서 다운로드한 데이터베이스와 프로그램 모듈을 저장한 다음 네트워크 트래픽을 줄일 수 있도록 네트워크의 다른 컴퓨터에 액세스할 수 있는 권한을 부여할 수 있습니다.

데이터 및 온라인 활동 실시간 감시

카스퍼스키 안티 바이러스는 로컬 네트워크와 인터넷에 안전하게 접근할 수 있도록 보장할 뿐 아니라 악성 프로그램과 무단 접근으로부터 컴퓨터 데이터를 보호합니다.

보호된 개체는 다음 세 그룹으로 분류됩니다:

- 파일, 개인 데이터, 다른 리소스에 대한 접근 파라미터(사용자 이름 및 암호), 뱅킹 카드에 대한 정보 등. 이러한 개체는 파일 안티 바이러스, 사전 방역에 의해 실시간으로 감시됩니다..
- 컴퓨터에 설치된 프로그램과 운영 체제 개체. 이러한 개체는 메일 안티 바이러스, 웹 안티 바이러스, 메신저 안티 바이러스, 사전 방역에 의해 실시간으로 감시됩니다.
- 온라인 활동: 전자 결제 시스템, 스팸 및 바이러스 등으로부터 이메일 실시간 감시. 이러한 개체는 메일 안티 바이러스, 웹 안티 바이러스, 메신저 안티 바이러스, 안티 피싱에 의해 실시간으로 감시됩니다.

마법사 및 도구

컴퓨터 보안은 운영 체제 기능 및 취약점을 찾아낼 수 있는 전문적인 지식이 필요한 어려운 작업입니다. 또한 시스템 보안에 대한 정보의 규모와 다양성으로 인해 분석하고 처리하는 것이 쉽지 않습니다.

카스퍼스키 안티 바이러스 패키지에는 특정 작업을 쉽게 해결할 수 있도록 컴퓨터 보안을 제공하는 마법사 및 도구 집합이 포함되어 있습니다.

- 브라우저 보안 마법사, Microsoft Internet Explorer 브라우저 설정의 분석을 수행하고 기본적으로 보안 지점에서 평가함.
- 시스템 복구 마법사, 시스템의 악성 프로그램 개체의 흔적 제거.
- 개인정보보호 마법사, 시스템 내 사용자 활동 및 사용자 활동에 대한 정보를 수집하도록 하는 운영 체제 설정의 흔적 검색 및 제거.

- 응급 복구 디스크, 감염된 x86 호환 컴퓨터의 검사 및 치료. 감염 레벨이 안티 바이러스 프로그램 또는 악성 프로그램 제거 유틸리티로 컴퓨터를 치료할 수 없다고 판단되는 경우 이 프로그램을 사용해야 합니다.
- 취약점 검사, 컴퓨터 진단 수행 및 컴퓨터에 설치된 운영 체제 및 사용자 프로그램의 취약점 검색 수행.
- 보안 키보드, 키보드로 입력된 데이터 가로채기 방지.

프로그램의 지원 기능

카스퍼스키 안티 바이러스에는 다양한 지원 기능이 포함되어 있습니다. 이러한 기능들은 프로그램을 최신 상태를 유지하고, 그 기능을 확장하며, 프로그램을 사용하는 데 도움을 주기 위한 것입니다.

데이터 파일 및 리포트

프로그램이 작동되는 동안 각 감시 구성요소, 검사 작업 또는 프로그램 업데이트 작업에 대해 리포트가 작성됩니다. 이 리포트에는 수행된 활동 및 작업 결과가 포함되며, 이 리포트로 카스퍼스키 안티 바이러스의 각 구성요소가 어떤 역할을 하는지 자세하게 알 수 있습니다. 문제가 발생하는 경우에는 해당 리포트를 카스퍼스키 랩에 보내어 카스퍼스키 랩 전문가들이 문제를 자세하게 파악하여 신속하게 도움을 줄 수 있도록 할 수 있습니다.

카스퍼스키 안티 바이러스는 위험하다고 의심되는 모든 파일을 격리 저장소라고 하는 특별한 저장소 영역으로 보냅니다. 이런 파일은 컴퓨터에 영향을 주지 않도록 암호화된 형태로 저장됩니다. 이 개체에 바이러스가 있는지 검사하거나, 초기 위치로 보내거나, 삭제하거나, 사용자가 직접 격리 저장소에 파일을 추가할 수 있습니다. 바이러스 검사가 완료된 후 감염되지 않은 것으로 검증된 모든 파일은 원래 위치에 자동으로 보내집니다.

카스퍼스키 안티 바이러스에서 치료하거나 삭제한 개체의 사본은 백업 저장소에 저장됩니다. 파일 또는 감염 사진을 복구해야 하는 경우 이런 사본이 만들어집니다. 파일의 백업 사본도 감염되지 않도록 암호화된 형태로 저장됩니다.

백업 저장소에서 초기 위치로 파일을 복구하거나 사본을 삭제할 수 있습니다.

라이센스

카스퍼스키 안티 바이러스를 구매하는 것은 프로그램 사용, 프로그램 데이터베이스 업데이트로의 접근 및 지정된 기간 동안 고객 지원을 관리하는 카스퍼스키 랩의 라이센스 계약이 적용된다는 것을 의미합니다. 사용 약관 및 프로그램의 전체 기능에 필요한 기타 정보는 라이센스에 포함되어 있습니다.

라이센스 기능을 사용하여 현재 라이센스에 대한 자세한 정보를 얻고, 새 라이센스를 구매하고, 기존 라이센스를 갱신할 수 있습니다.

지원

카스퍼스키 안티 바이러스에 등록한 사용자는 기술 지원 서비스에 연락할 수 있습니다. 서비스 조건에 대한 자세한 내용을 보려면 지원 옵션을 사용하십시오.

제공되는 링크를 사용하여 카스퍼스키 랩 제품 사용자 포럼에 접근하거나, 고객 지원에 오류 리포트를 보내거나, 특정 온라인 양식을 작성하여 프로그램에 대한 의견을 보낼 수 있습니다.

온라인 고객 지원 및 개인 사용자 캐비닛 서비스에 문의할 수도 있습니다. 카스퍼스키 안티 바이러스 전문가들은 카스퍼스키 안티 바이러스에 대한 전화 지원을 항상 즐거운 마음으로 제공하고 있습니다.

카스퍼스키 안티 바이러스 설치

카스퍼스키 안티 바이러스는 대화형 모드에서 프로그램 설치 마법사를 사용하여 설치됩니다.

설치 전에 모든 실행중의 응용 프로그램을 종료할 것을 권합니다.

컴퓨터에 카스퍼스키 안티 바이러스를 설치하려면 배포 파일을 실행합니다 (*.exe 확장자를 가진 파일).

인터넷에서 다운로드한 파일로 프로그램을 설치하는 것은 CD의 파일로 설치하는 것과 완전히 같습니다.

설치 후, 마법사는 프로그램 설치 패키지 (*.msi 확장자의 파일)를 찾기 위해 검색을 하며, 만약 이러한 파일이 발견되면 마법사는 카스퍼스키 랩의 인터넷 서버에서 새로운 버전을 찾기 위해 검색을 할 것입니다. 만약 설치 패키지 파일이 발견되지 않았을 경우, 다운로드를 하도록 안내합니다. 파일이 다운로드 된 후, 프로그램 설치가 시작됩니다. 만약 다운로드를 취소하면, 프로그램 설치 과정은 보통 모드로 재개됩니다.

설치 프로그램은 마법사로 구성되어 있습니다. 각각의 창은 설치 과정을 제어하기 위한 버튼을 포함하고 있습니다. 아래에는 이들의 용도를 간단하게 설명합니다:

- **다음** – 행동을 받아들이고 설치 다음 단계로 계속.
- **이전** – 설치 과정의 이전 단계로 돌아갑니다.
- **취소** – 설치를 취소합니다.
- **완료** – 프로그램 설치 과정을 완료합니다.

설치 과정의 각 단계에 대하여 자세히 확인합니다.

참조:

1 단계. 새 버전의 프로그램 검색 24

2 단계. 설치 조건에 시스템이 부합하는지 확인 24

3 단계. 설치 유형 선택 24

4 단계. 최종 사용자 동의서 25

5 단계. 카스퍼스키 시큐리티 네트워크에 참가 25

6 단계. 설치 폴더 선택 25

7 단계. 설치할 프로그램 구성요소 선택 25

8 단계. 설치 후에 저장된 프로그램 설정 사용 26

9 단계. 다른 안티 바이러스 프로그램 검색 26

10 단계. 설치 최종 준비 27

11 단계. 설치 완료 27

1 단계. 새 버전의 프로그램 검색

프로그램을 컴퓨터에 설치하기 전에, 마법사는 카스퍼스키 랩의 업데이트 서버를 검색하여 설치할 프로그램의 새로운 버전이 존재하는지 확인합니다.

만약 카스퍼스키 랩 업데이트 서버에 새로운 버전이 발견되지 않는다면, 설치 마법사는 현재 버전의 설치를 시작합니다.

만약 프로그램의 새로운 버전이 서버에서 발견되면 이 다운로드가 제공됩니다. 만약 다운로드를 취소하면, 설치 마법사는 현재 버전의 설치를 시작합니다. 만약 새로운 버전의 설치를 선택하면, 설치 파일이 컴퓨터로 다운로드 되며, 설치 마법사는 자동적으로 새로운 버전의 설치를 시작하게 됩니다. 새로운 버전의 설치에 관한 더 많은 정보는 상응되는 프로그램 버전의 문서를 참조하십시오.

2 단계. 설치 조건에 시스템이 부합하는지 확인

컴퓨터에 프로그램을 설치하기 전에, 마법사는 운영 체제와 설치되어 있는 서비스 팩이 소프트웨어 설치 조건에 부합하는지 확인합니다. 또한 필요한 프로그램이 컴퓨터에 설치되어 있는지, 그러한 소프트웨어를 설치할 권한이 있는지 확인합니다.

만약 어떠한 조건에 부합하지 않는다면, 상응하는 알림이 화면에 표시됩니다. 카스퍼스키 랩의 프로그램을 설치하기 전에 Windows Update 서비스를 이용하여 필요한 업데이트와 프로그램을 설치하는 것을 권장합니다.

3 단계. 설치 유형 선택

시스템이 요구 사항에 맞고 프로그램의 새 버전이 카스퍼스키 랩 업데이트 서버에 없거나 여러부니 새 버전 설치를 취소했다면설치 현재 버전의 카스퍼스키 안티 바이러스 설치 마법사가 실행될 것입니다.

이 단계에서는 가장 적합한 설치 유형을 선택하게 됩니다:

- *빠른 설치*. 만약 이 옵션을 선택하면(☐ **수동 설치** 체크박스 해제), 모든 프로그램이 카스퍼스키 랩의 전문가 권장 설정과 함께 컴퓨터에 설치됩니다. 설치가 완료된 후 프로그램 설치 마법사가 시작됩니다.
- *사용자 지정 설치*. 이 경우에는(☐ **수동 설치** 체크박스 선택), 컴퓨터에 설치하기를 원하는 구성요소와 프로그램이 설치될 폴더를 선택하게 되며, 설치 마법사를 사용하여 프로그램을 활성화하여 설정하게 됩니다

- 만약 첫 번째 옵션을 선택했을 경우, 프로그램 설치 마법사는 라이센스 동의와 카스퍼스키 시큐리티 네트워크 데이터 제공 단계로 진행됩니다. 그후 시스템에 설치가 시작될 것입니다.
- 두 번째 옵션을 선택했을 경우, 다른 모든 경우에는 설치 다음 단계로 넘어가는 때 사용자의 확인이 필요합니다.
- 설치를 계속하기 위하여 **다음** 버튼을 클릭합니다. 설치를 취소하려면 **취소** 버튼을 클릭합니다.

4 단계. 최종 사용자 동의서

다음 마법사 대화 창은 사용자와 카스퍼스키랩의 저작권 동의서를 표시합니다. 자세히 읽고, 모든 조건과 내용에 동의한다면 '**동의**'를 선택하고 다음 버튼을 누릅니다. 설치가 계속될 것 입니다.

설치를 취소하려면 **취소** 버튼을 누릅니다.

5 단계. 카스퍼스키 시큐리티 네트워크 데이터 수집 성명

이 단계에서, 사용자는 카스퍼스키의 시큐리티 네트워크 프로그램에 참가할 수 있습니다. 카스퍼스키 시큐리티 네트워크는 잠재적 위협에 대한 보안과 프로그램에 관한 정보를 수집하여 분석을 위해 카스퍼스키 랩으로 전송합니다. 이러한 정보는 개인 확인을 위한 정보를 전혀 담고 있지 않으며, 보안 향상과 악성 보안위협, 바이러스에 대한 강화된 대응을 위해서만 카스퍼스키랩에서 이용됩니다.

카스퍼스키 시큐리티 네트워크 수집 성명을 보고 동의하신다면, ☐ **성명서를 읽었으며, 카스퍼스키 시큐리티 네트워크에 참가하겠습니다.** 에 체크 합니다.

설치를 계속하려면 **다음** 버튼을 누릅니다.

6 단계. 설치 폴더 선택

이 설치 마법사 단계는 사용자 프로그램 설치를 선택했을 경우에만 실행됩니다.

이 단계에서는 컴퓨터에서 프로그램이 설치될 폴더를 선택하게 됩니다. 기본 경로는 다음과 같습니다:

- **<drive> ₩ Program Files ₩ Kaspersky Lab ₩ Kaspersky Anti-Virus 2010** – 32 비트 시스템.
- **<drive> ₩ Program Files (x86) ₩ Kaspersky Lab ₩ Kaspersky Anti-Virus Security 2010** –64 비트 시스템.

찾기 버튼을 누르고 기존 폴더를 대화 창에서 선택하거나, 입력란에 경로를 입력하여 다른 폴더를 지정할 수 있습니다.

설치 폴더로의 전체 경로를 수동으로 입력한 경우, 경로의 길이는 200자를 넘어서는 안되며 특수 문자를 포함할 수 없습니다.

설치를 계속하려면 **다음** 버튼을 누릅니다.

7 단계. 설치할 프로그램 구성요소 선택

이 단계는 사용자 지정 설치 옵션을 선택할 경우에만 실행됩니다.

사용자 지정 설치의 경우, 컴퓨터에 설치를 원하는 카스퍼스키 안티 바이러스의 구성요소를 선택해야 합니다. 설치 시, 기본적으로 실시간 감시 구성요소, 검사 작업과 업데이트 작업을 포함해 모든 카스퍼스키 안티 바이러스 구성요소가 선택되어 있습니다.

어떤 구성요소를 설치하고 싶은지 결정하려면 각 구성요소에 관한 간단한 정보를 참고할 수 있습니다. 목록에서 원하는 구성요소를 선택하고 그것에 관한 정보를 아래 설명 칸에서 읽을 수 있습니다. 이 정보에는 구성요소의 목적과 설치에 필요한 디스크 공간에 대한 간단한 설명이 포함되어 있습니다.

컴포넌트의 설치를 취소하려면 설정 메뉴의 컴포넌트 이름 옆의 아이콘을 클릭하여 나타나는 설정 메뉴에서 **전체 기능을 이용할 수 없게 됩니다**를 선택합니다. 일부 컴포넌트를 설치하지 않으면 다른 위험한 프로그램들로부터 보호되지 않을 수 있습니다.

설치할 구성요소를 선택하려면 컴포넌트 이름 옆의 아이콘을 클릭하여 나타나는 설정 메뉴에서 **이 기능을 로컬 하드 드라이브에서 설치합니다**를 선택합니다.

설치할 컴포넌트 선택을 끝냈다면 **다음** 버튼을 클릭합니다. 설치되는 구성요소의 기본 목록으로 돌아가려면 **초기화** 버튼을 클릭합니다.

8 단계. 이전 설치 시에 저장된 프로그램 설정 사용

이 단계에서 사용자는 카스퍼스키 이전 버전을 제거하면서 전에 사용하였던 설정(프로그램의 보호 설정 및 데이터베이스, 안티 스팸의 데이터베이스)을 사용할 지 선택할 수 있습니다.

위에 설명된 내용이 어떻게 적용되는지 자세히 살펴봅니다.

만약 사용자의 컴퓨터에 카스퍼스키 안티 바이러스의 이전 버전이 설치되었다면, 그것이 삭제되고 난 뒤에도 프로그램 데이터베이스는 저장되어있기 때문에 설치되는 버전과 호환될 수 있습니다. 이렇게 하려면 ☐ **프로그램 데이터베이스** 박스에 체크합니다. 설치 패키지에 포함된 데이터베이스는 컴퓨터에 복사되지 않을 것입니다.

컴퓨터에 저장된 이전 버전의 설정을 사용하려면 ☐ **이전 버전에서 저장된 프로그램 설정**에 체크합니다.

9 단계. 다른 안티 바이러스 프로그램 검색

이 단계에서 마법사는 카스퍼스키 안티 바이러스와의 충돌을 일으킬 수 있는 카스퍼스키 랩의 프로그램을 포함한 다른 안티 바이러스 프로그램을 검색합니다.

그러한 프로그램이 컴퓨터에서 발견된 경우, 그 목록들이 화면에 표시됩니다. 설치를 계속하기 전에 이들을 삭제하도록 권장합니다.

사용자는 발견된 안티 바이러스 프로그램의 목록을 통하여 삭제 모드(자동 또는 수동)를 선택 할 수 있습니다.

발견된 안티 바이러스 프로그램 목록에 카스퍼스키랩의 2009 버전 프로그램이 있다면 사용자는 수동으로 삭제할 때, 키 파일을 저장할 수 있습니다. 그리고 이 키파일을 새로운 버전에서 사용할 수 있습니다. 또한 사용자는 격리 및 백업 개체를 저장할 수 있도록 알림을 받게 됩니다. 그 개체들은 자동으로 카스퍼스키 안티 바이러스의 업데이트 된 버전의 격리 저장소에 저장되고 그것들에 대한 작업도 지속할 수 있게 됩니다.

만약 2009 버전을 자동으로 삭제된다면 활성화 정보가 저장될 것이며 2010 버전 설치 시 사용될 것입니다.

작업이 완료되면 **다음** 버튼을 누릅니다.

10 단계. 설치 최종 준비

이 단계에서는 컴퓨터에서 설치를 위한 준비를 완료하게 됩니다.

초기 및 사용자 지정 설치 시, ☐ **설치 중 자기-보호 사용**을 그대로 두는 것을 권장합니다. 설치 중 에러가 발생할 경우, 자기-보호 기능은 설치 롤백의 올바른 절차를 수행할 수 있도록 할 것입니다. 설치를 다시 시도할 때 이 박스의 체크를 해제할 것을 권장합니다.

원격 데스크톱을 통한 프로그램의 원격 설치의 경우, ☐ **설치 중 자기-보호 사용** 박스의 체크를 해제할 것을 권장합니다. 이 박스를 체크한 경우, 설치 과정이 완료되지 않게 되거나 아예 진행되지 않을 수 있습니다.

설치를 계속하려면 **설치** 버튼을 누릅니다.

네트워크 트래픽을 감시하는 카스퍼스키 안티 바이러스 구성 요소를 설치할 때 네트워크 연결이 끊길 수 있습니다. 시간이 조금 지난 후 대부분의 끊긴 연결이 복구될 것입니다.

11 단계. 설치 완료

설치 완료 창은 컴퓨터에 카스퍼스키 안티 바이러스 설치 완료에 대한 정보를 담고 있습니다.

다음 단계는 컴퓨터에 저장되는 정보의 최대의 보호를 확실히 하기 위한 프로그램 설정입니다. 설정 마법사는 카스퍼스키 안티 바이러스를 빠르고 정확하게 설정하도록 돕습니다.

프로그램 설정으로 전환하려면 **다음** 버튼을 누릅니다.

시작하기

카스퍼스키 안티 바이러스 개발 시 카스퍼스키 랩에서 중점을 둔 요소 중 하나는 프로그램을 최적으로 구성하는 것입니다. 따라서 컴퓨터 사용 수준에 관계없이 카스퍼스키 안티 바이러스 설치 후 설정에 시간을 들이지 않고 즉시 컴퓨터를 감시할 수 있습니다.

사용자의 편의를 위해 프로그램 구성 마법사의 통합된 인터페이스에 예비 구성 단계를 도입하여 프로그램 설치 절차가 완료됨과 동시에 시작되도록 했습니다. 마법사의 안내를 따라 카스퍼스키 안티 바이러스를 활성화하고 업데이트 설정을 수정하며 암호를 사용하여 프로그램 접근을 차단하고 기타 설정을 편집할 수 있습니다.

카스퍼스키 안티 바이러스를 설치하기 전에 컴퓨터가 이미 악성 프로그램에 감염되어 있을 수도 있습니다. 악성 프로그램을 탐지하려면 컴퓨터 전체 검사를 실행합니다.

악성 프로그램이 작동되고 시스템에 오류가 발생하면 컴퓨터 설정이 손상될 수 있습니다. 설치된 소프트웨어의 취약점 및 시스템 설정의 잘못된 부분을 발견하려면 취약점 검사 작업을 실행합니다.

프로그램을 설치할 시점에 설치 패키지에 포함된 데이터베이스가 매우 오래되었을 수 있습니다. 따라서 프로그램 업데이트를 실행합니다. 설치 마법사를 통해 또는 프로그램 설치 직후 자동으로 수행된 경우는 업데이트가 필요 없습니다.

카스퍼스키 안티 바이러스 패키지에 포함된 안티 스팸 구성요소는 자기-학습 알고리즘을 사용하여 원하지 않는 메시지를 탐지합니다. 메일 작업에 대한 구성요소를 구성하려면 안티 스팸 학습 마법사를 실행합니다.

위에서 설명한 작업을 완료했으면 카스퍼스키 안티 바이러스를 작동할 수 있습니다. 컴퓨터 감시 수준을 평가하려면 보안 관리 마법사를 사용합니다.

참조:

프로그램 구성 마법사 29

프로그램 업데이트 33

컴퓨터 바이러스 검사 33

컴퓨터 취약점 검사 34

라이센스 관리 34

자동 라이센스 갱신 신청 35

카스퍼스키 시큐리티 네트워크 참가 36

보안 관리 37

실시간 감시 상태 39

감시 일시 중지 40

프로그램 구성 마법사

프로그램 구성 마법사는 설치가 완료된 후 시작되어 컴퓨터의 기능 및 작업에 따라 프로그램 초기 설정 편집을 도와 줍니다.

프로그램 구성 마법사 인터페이스는 **뒤로** 및 **다음** 링크를 사용하여 이동하는 일련의 창(단계)으로 구성됩니다. 마법사를 닫으려면 **취소** 버튼을 사용합니다.

마법사 단계에 대한 상세한 정보

1 단계. 프로그램 활성화 29

2 단계. 감시 모드 선택 31

3 단계. 프로그램 업데이트 구성 31

4 단계. 프로그램 접근 차단 32

5 단계. 탐지할 보안위협 선택 32

6 단계. 마법사 종료 33

1 단계. 프로그램 활성화

프로그램 활성화 절차는 라이센스 키 파일을 설치하여 라이센스를 등록하는 것입니다. 카스퍼스키 안티 바이러스는 라이센스에 따라 기존 권한을 확인하고 사용 기간을 계산합니다.

라이센스 키 파일에는 카스퍼스키 안티 바이러스가 전체 기능으로 작동하는 데 필요한 서비스 정보와 다음과 같은 데이터가 포함되어 있습니다:

- 지원 정보(지원 공급자 및 지원 위치);
- 라이센스 키 파일 이름 및 번호, 라이센스 만료 날짜.

프로그램을 활성화하려면 인터넷 연결이 필요합니다.

활성화 시 라이센스 키 파일을 얻으려면 활성화코드가 있어야 합니다. 활성화코드는 프로그램 구입 시 제공됩니다. 다음과 같은 카스퍼스키 안티 바이러스 활성화 옵션이 주어집니다:

- **상업용 라이센스 활성화.** 상업용 버전의 프로그램을 구입하고 활성화코드를 받은 경우 이 활성화 옵션을 선택합니다. 활성화코드를 사용하여 라이센스 키 파일을 받으면 전체 라이센스 기간 동안 프로그램의 모든 기능을 사용할 수 있습니다.

- **체험판으로 활성화.** 상업용 버전 구입을 결정하기 전에 체험판 프로그램을 설치하려면 이 활성화 옵션을 사용합니다. 체험판 라이센스 계약에 지정된 기간 동안 유효한 무료 라이센스 키 파일을 받게 됩니다.

- **나중에 활성화.** 이 옵션을 선택하면 카스퍼스키 안티 바이러스 활성화 단계를 건너뜁니다. 프로그램이 컴퓨터에 설치되고 업데이트를 제외한 프로그램의 모든 옵션을 사용할 수 있습니다. 설치 후에 단 한 번만 카스퍼스키 안티 바이러스를 업데이트할 수 있습니다. 나중에 활성화 옵션은 프로그램 설치 직후 활성화 마법사를 처음 시작할 때만 사용할 수 있습니다.

카스퍼스키 안티 바이러스를 설치한 다음 활성화 정보를 저장한 상태로 제거하면 이 단계를 건너뜁니다. 이 경우 구성 마법사는 자동으로 기존 라이센스에 대한 정보를 받습니다. 이 정보는 마법사 창에 표시됩니다.

참조:

상업용 버전 활성화 30

체험판 버전 활성화 31

활성화 완료 31

상업용 버전 활성화

이 옵션을 선택하면 카스퍼스키 랩 서버에서 프로그램이 활성화되므로 인터넷 연결이 필요합니다.

활성화는 인터넷을 통해 카스퍼스키 안티 바이러스를 구입할 때 이메일로 받은 활성화코드를 입력하여 수행됩니다. 일반 정품 버전으로 프로그램을 구입한 경우 활성화코드는 활성화 카드에 인쇄되어 있습니다.

활성화코드는 공백 없이 하이픈으로 구분된 네 개의 그룹으로서 각 그룹이 다섯 자리로 이루어져 있습니다(예: 11111-11111-11111-11111). 코드는 라틴 문자로만 입력해야 합니다.

활성화 마법사는 인터넷을 통해 카스퍼스키 랩의 활성화 서버와 연결하여 사용자의 활성화코드를 보냅니다. 그런 다음 활성화코드가 확인됩니다. 활성화코드 확인이 성공하면 마법사에서 라이센스 키 파일을 받아 자동으로 설치합니다. 활성화 프로세스가 완료되면서 구입한 라이센스에 대한 자세한 정보가 담긴 창이 표시됩니다.

라이센스(subsctiption)를 활성화했으면 위의 정보와 함께 라이센스(subscription) 상태에 대한 정보가 표시됩니다.

활성화코드 확인이 실패하면 해당 메시지가 화면에 표시됩니다. 이 경우 카스퍼스키 안티 바이러스를 구입한 소프트웨어 공급업체에 문의하여 자세한 정보를 확인해야 합니다.

활성화코드를 사용하여 허용된 인증 횟수를 초과하면 이를 알리는 팝업 메시지가 화면에 표시됩니다. 활성화 프로세스가 중단되고 카스퍼스키 랩의 기술 지원 서비스에 문의하라는 메시지가 나타납니다.

활성화 서버에 연결하는 동안 오류가 발생하고 라이센스 키 파일을 받을 수 없는 경우 기술 지원 서비스에 문의하십시오.

체험판 버전 활성화

카스퍼스키 안티 바이러스 체험판 프로그램을 설치해 본 다음 상업용 버전의 구입을 결정하려면 이 활성화 옵션을 사용합니다. 체험판 라이센스 계약에 지정된 기간 동안 유효한 무료 라이센스 키 파일을 받게 됩니다. 체험판 라이센스는 만료 후 다시 활성화할 수 없습니다.

활성화 서버에 연결하는 동안 오류가 발생하고 라이센스 키 파일을 받을 수 없는 경우 기술 지원 서비스에 문의하십시오.

활성화 완료

활성화 마법사에 카스퍼스키 안티 바이러스가 성공적으로 활성화되었다는 메시지가 나타납니다. 또한 라이센스 형태(상업용, 체험판 등), 만료 날짜, 라이센스당 호스트 수와 같은 라이센스에 대한 정보가 표시됩니다.

라이센스(subscription)를 활성화했으면 라이센스 키 만료 날짜 대신 라이센스(subscription) 상태에 대한 정보가 표시됩니다.

2 단계. 감시 모드 선택

카스퍼스키 안티 바이러스에서 제공하는 감시 모드를 선택합니다.

두 가지 모드를 사용할 수 있습니다:

- *자동.* 중요한 이벤트가 발생할 경우 카스퍼스키 안티 바이러스가 카스퍼스키 랩에서 권장하는 처리 방법을 자동으로 수행합니다. 보안위협이 탐지되면 해당 개체를 치료하려고 시도하며, 치료에 실패할 경우 개체를 삭제합니다. 감염의심 개체는 처리 없이 건너뜁니다. 새로운 이벤트가 발생하면 이를 알리는 팝업 메시지가 나타납니다.
- *대화식.* 이 모드에서는 카스퍼스키 안티 바이러스가 사용자가 지정한 방식으로 이벤트에 반응합니다. 사용자의 주의가 필요한 이벤트가 발생할 경우 알림이 표시되어 처리 방법을 선택할 수 있습니다.

처리 안된 감염이 탐지될 경우 선택한 감시 모드에 관계없이 알림이 표시됩니다.

3 단계. 프로그램 업데이트 구성

빠른 설치 모드를 선택한 경우 프로그램 구성 마법사의 이 단계는 건너뜁니다. 이 단계에서 편집한 프로그램 설정은 기본값으로 할당됩니다.

컴퓨터 감시 품질은 데이터베이스 및 프로그램 모듈의 정기적인 업데이트에 직접적으로 좌우됩니다. 이 구성 마법사 창에서는 카스퍼스키 안티 바이러스 업데이트 모드를 선택하고 스케줄 설정을 편집합니다.

- **자동 업데이트**. 카스퍼스키 안티 바이러스가 업데이트 경로에서 업데이트 패키지가 있는지 지정된 간격으로 확인합니다. 검사 빈도는 안티 바이러스 급증 시 늘어날 수 있고 반대의 경우 줄어들 수 있습니다. 새 업데이트가 발견되면 컴퓨터에 다운로드하여 설치합니다. 기본 처리 방법입니다.

- **스케줄 업데이트**(시간 간격은 스케줄 설정에 따라 달라질 수 있음). 생성된 스케줄에 따라 업데이트가 자동으로 실행됩니다. 설정 버튼을 누르면 열리는 창에서 스케줄 설정을 변경할 수 있습니다.

- **수동 업데이트**. 이 옵션을 선택할 경우 프로그램 업데이트를 사용자가 직접 실행합니다.

카스퍼스키 안티 바이러스를 설치할 시점에는 설치 패키지에 포함된 데이터베이스 및 프로그램 모듈이 매우 오래될 수 있습니다. 따라서 카스퍼스키 안티 바이러스의 최신 업데이트를 받는 것이 좋습니다. 이렇게 하려면 **지금 업데이트** 버튼을 누릅니다. 그러면 업데이트 서버에서 필요한 업데이트가 다운로드되어 컴퓨터에 설치됩니다.

설치 패키지에 포함된 데이터베이스가 매우 오래된 경우 업데이트 패키지가 커서 인터넷 트래픽이 최대 수십 MB까지 증가할 수 있습니다.

업데이트 설정 편집(업데이트 다운로드 경로와 업데이트 프로세스를 실행하는 데 사용할 사용자 계정을 선택한 다음 로컬 경로로의 업데이트 배포 서비스 작동)으로 이동하려면 설정 버튼을 누릅니다.

4 단계. 프로그램 접근 차단

빠른 설치 모드를 선택한 경우 카스퍼스키 안티 바이러스 구성 마법사의 이 단계는 건너뜁니다. 이 단계에서 편집한 프로그램 설정은 기본값으로 할당됩니다.

컴퓨터 사용 수준이 사용자마다 다르고 악성 프로그램이 실시간 감시를 중지할 수 있으므로 카스퍼스키 안티 바이러스 프로그램에 암호를 지정하여 접근하는 옵션이 제공됩니다. 암호를 사용하면 임의로 실시간 감시를 중지하거나 카스퍼스키 안티 바이러스 설정을 변경하지 못하도록 차단됩니다.

암호 보호를 작동하려면 ☐ **암호 보호 작동** 상자를 체크하고 **새로운 암호**와 **새로운 암호 확인** 칸에 암호를 입력합니다.

아래에 암호로 보호하려는 영역을 지정합니다:

- ☐ **프로그램 설정 구성** – 사용자가 카스퍼스키 안티 바이러스 설정에 대한 변경 사항을 저장하려고 하면 암호를 요구합니다.

- ☐ **프로그램 종료** – 사용자가 프로그램을 종료하려고 하면 암호를 요구합니다.

5 단계. 탐지할 보안위협 선택

빠른 설치 모드를 선택한 경우 프로그램 구성 마법사의 이 단계는 건너뜁니다. 이 단계에서 편집한 프로그램 설정은 기본값으로 할당됩니다.

이 단계에서는 카스퍼스키 안티 바이러스에서 탐지할 보안위협 카테고리를 선택할 수 있습니다. 바이러스, 웜, 트로이목마 등을 비롯한 컴퓨터를 손상시킬 수 있는 프로그램은 카스퍼스키 안티 바이러스에서 항상 탐지합니다.

6 단계. 마법사 종료

마법사의 마지막 창에서는 프로그램 설치가 성공적으로 완료되었음을 알립니다. 카스퍼스키 안티 바이러스를 실행하려면 ☐ **카스퍼스키 안티 바이러스 실행** 상자를 체크하고 **마침** 버튼을 누릅니다.

프로그램 업데이트

카스퍼스키 안티 바이러스를 업데이트하려면 인터넷 연결이 필요합니다.

카스퍼스키 안티 바이러스는 프로그램 데이터베이스를 사용하며 여기에는 보안위협 서명, 스팸에 일반적인 문구 및 네트워크 공격에 대한 설명이 포함되어 있습니다. 카스퍼스키 랩은 데이터베이스와 프로그램 모듈을 모두 정기적으로 업데이트하기 때문에 카스퍼스키 안티 바이러스가 설치되는 시점에는 이러한 데이터베이스가 매우 오래되어 있을 수 있습니다.

프로그램 구성 마법사를 사용하는 경우 업데이트 실행 모드를 선택할 수 있습니다. 기본적으로 카스퍼스키 안티 바이러스는 카스퍼스키 랩의 업데이트 서버에서 업데이트를 자동으로 확인합니다. 서버에 새로운 업데이트가 포함되어 있는 경우 다운로드되어 무인 모드로 설치됩니다.

설치 패키지에 포함된 데이터베이스가 매우 오래된 경우 업데이트 패키지가 커서 인터넷 트래픽이 최대 수십 MB까지 증가할 수 있습니다.

컴퓨터의 실시간 감시를 최신 상태로 유지하도록 설치 후에 즉시 카스퍼스키 안티 바이러스를 업데이트하는 것이 좋습니다.

- *카스퍼스키 안티 바이러스를 수동으로 업데이트하려면 다음과 같이 하십시오:*

  1. 메인 프로그램 창을 엽니다.
  2. 창 왼쪽에서 **업데이트 센터** 섹션을 선택합니다.
  3. **업데이트 시작** 버튼을 누릅니다.

컴퓨터 바이러스 검사

악성 프로그램 개발자들은 사용자가 컴퓨터에서 악성 프로그램의 존재를 눈치치지 못하도록 해당 프로그램 작업을 숨기려고 애씁니다.

카스퍼스키 안티 바이러스는 설치 후에 자동으로 컴퓨터에 대한 **빠른 검사**를 수행합니다. 이 작업을 통해 운영 체제 시작 시 로드되는 개체에서 유해한 프로그램을 검색하여 처리합니다.

카스퍼스키 랩 전문가들은 또한 **전체 검사** 작업을 수행할 것을 권장합니다.

- *바이러스 검사 작업을 시작하려면 다음과 같이 하십시오:*

  1. 메인 프로그램 창을 엽니다.
  2. 창 왼쪽에서 **수동 검사** 섹션을 선택합니다.
  3. **컴퓨터 전체 검사 시작** 버튼을 눌러 검사를 시작합니다.

컴퓨터 취약점 검사

시스템 오류 또는 악성 프로그램 활동으로 인해 운영 체제 설정이 손상될 수 있습니다. 또한 컴퓨터에 설치된 사용자 프로그램에 취약점이 있어 침입자가 이를 이용해 컴퓨터를 손상시킬 수도 있습니다.

이러한 프로그램을 탐지하여 제거하려면 카스퍼스키 안티 바이러스를 설치한 후 취약점 검사 작업을 실행하는 것이 좋습니다. 검사 작업 중에는 설치된 프로그램의 취약점은 물론 운영 체제와 브라우저 설정의 손상 및 잘못된 부분이 있는지도 검색합니다.

- *취약점 검사 작업을 시작하려면 다음과 같이 하십시오:*

  1. 메인 프로그램 창을 엽니다.
  2. 창 왼쪽에서 **수동 검사** 섹션을 선택합니다
  3. **내 컴퓨터 및 취약점이 있는 소프트웨어가 있는지 검사합니다.** 버튼을 누릅니다.
  4. 열리는 창에서 **취약점 검사 시작** 버튼을 누릅니다.

라이센스 관리

카스퍼스키 안티 바이러스를 작동하려면 유효한 라이센스 키가 필요합니다. 라이센스 키 파일은 카스퍼스키 안티 바이러스 구입 시 제공된 활성화코드를 사용하여 받게 되며, 활성화 날짜부터 제품을 사용할 수 있는 권한을 부여합니다. 라이센스 키 파일에는 라이센스 형태, 만료 날짜, 호스트 수와 같은 라이센스에 대한 정보가 들어 있습니다.

라이센스 키 파일 없이는 체험판 버전을 활성화하지 않는 한 카스퍼스키 안티 바이러스에서 한 번의 업데이트만 가능하며 새로운 업데이트가 다운로드되지 않습니다.

체험판 버전을 활성화한 경우 체험판 사용 기간이 만료된 후에는 프로그램이 실행되지 않습니다.

상업용 버전의 라이센스가 만료된 경우 프로그램은 계속 작동하지만 데이터베이스가 업데이트되지 않습니다. 즉, 이전과 같이 컴퓨터에서 바이러스를 검사하고 실시간 감시 구성요소를 사용할 수 있지만 라이센스 만료 전에 있던 데이터베이스가 사용되므로 라이센스 만료 후에는 컴퓨터가 바이러스로부터 보호되는 것을 보장할 수 없습니다.

컴퓨터가 신종 바이러스에 감염되지 않도록 하려면 카스퍼스키 안티 바이러스 라이센스를 갱신하는 것이 좋습니다. 라이센스가 만료되기 2 주 전부터 만료 사실을 알려 얼마 동안 프로그램을 실행할 때마다 관련 메시지가 표시됩니다.

현재 사용 중인 라이센스에 대한 정보는 라이센스 관리 창에서 확인할 수 있습니다. 라이센스 형태(상업용, 상업용 라이센스(subscription), 상업용 보호 라이센스(subscription), 체험판), 최대 호스트 수, 만료 날짜 및 남은 날짜가 표시됩니다. 상업용 라이센스(subscription) 또는 상업용 보호 라이센스(subscription)가 설치된 경우 라이센스 만료에 대한 정보가 표시되지 않습니다.

프로그램 라이센스 동의서 조항을 보려면 **최종 사용자 라이센스 동의서 보기** 버튼을 누릅니다. 라이센스 키 파일을 삭제하려면 라이센스 키 파일을 삭제하려는 라이센스 오른쪽에 있는 ☐ 버튼을 누릅니다. 새로운 라이센스를 활성화하려면 **새로운 라이센스 활성화** 버튼을 누릅니다.

라이센스 구매(라이센스 갱신) 버튼을 사용하면 카스퍼스키 랩 온라인 스토어에서 라이센스를 구입(갱신)할 수 있습니다.

카스퍼스키 랩에서는 제품 라이센스 연장에 대해 특별 가격 혜택을 정기적으로 제공하고 있습니다. 특별 혜택에 대한 정보는 카스퍼스키 랩 웹사이트를 참조하십시오.

자동 라이센스 갱신 신청

라이센스(subscription)를 사용하면 라이센스가 자동으로 갱신됩니다. 라이센스(subscription)를 활성화하려면 카스퍼스키 안티 바이러스 구입 시 온라인 스토어에서 받은 활성화코드가 필요합니다.

라이센스(subscription) 활성화 시점에 제한된 기간의 라이센스가 이미 활성화되어 있는 경우 라이센스(subscription)로 대체됩니다. 라이센스(subscription)를 취소하려면 제품을 구입한 온라인 스토어에 문의하십시오.

라이센스(subscription) 상태는 다음 옵션을 사용하여 지정됩니다:

- *정의 중.* 라이센스(subscription)를 활성화하려는 요청이 처리되지 않았습니다. 서버에서 요청을 처리하는 데 어느 정도 시간이 필요합니다. 카스퍼스키 안티 바이러스의 모든 기능이 작동합니다. 일정 기간이 지난 후 라이센스(subscription) 요청이 처리되지 않는 경우 라이센스(subscription) 상태 업데이트가 수행되지 않았다는 알림을 받게 됩니다. 이 경우 라이센스(subscription)에 대해 프로그램 데이터베이스가 더 이상 업데이트되지 않고 보호 라이센스(subscription)에 대해 컴퓨터 감시가 수행되지 않습니다.
- *활성화 됨.* 라이센스(subscription)가 정해진 기간 없이 활성화되었거나 일정 기간 동안(만료 날짜 정의됨) 활성화되었습니다.
- *갱신 됨.* 라이센스(subscription)가 정해진 기간 없이 갱신되었거나 일정 기간 동안 갱신되었습니다.
- *오류.* 라이센스(subscription) 상태를 업데이트하는 동안 오류가 발생했습니다.
- *만료 됨. 유예기간.* 라이센스(subscription)가 만료되었거나 상태 갱신 기간이 만료되었습니다. 상태 갱신 기간이 만료된 경우 라이센스(subscription) 상태를 수동으로 업데이트해야 합니다. 라이센스(subscription)가

만료된 경우 카스퍼스키 안티 바이러스를 구입한 온라인 스토어에 문의하여 갱신할 수 있습니다. 다른 활성화코드를 사용하려면 먼저 현재 사용 중인 라이센스(subscription) 키 파일을 삭제해야 합니다.

- *만료됨. 유예 기간 만료됨.* 라이센스(subscription)가 만료되었거나 상태 갱신 유예 기간이 만료되었습니다. 새로운 라이센스(subscription)를 구입하거나 기존 라이센스(subscription)를 갱신하려면 판매처 쇼핑몰에 문의하십시오.
- *라이센스 취소.* 자동 라이센스 갱신을 위한 라이센스(subscription)를 취소합니다.
- *업데이트 필요.* 어떠한 이유로 라이센스(subscription) 상태가 적절한 시점에 업데이트되지 않았습니다. 라이센스(subscription) 상태를 업데이트하려면 **라이센스(subscription) 상태 업데이트** 버튼을 사용합니다.
- *일시중지.* 자동 라이센스 갱신에 대한 라이센스(subscription)가 일시 중지되었습니다.
- *다시 시작됨.* 라이센스(subscription)가 다시 시작되었습니다.

라이센스(subscription) 유효 기간과 라이센스를 갱신할 수 있는 유예 기간이 모두 경과한 경우(라이센스(subscription) 상태 – *만료됨*) 카스퍼스키 안티 바이러스에서 이를 알리고 라이센스 자동 갱신 시도를 중지합니다. 라이센스(subscription)의 경우 프로그램 기능은 그대로 유지되지만 데이터베이스 업데이트 기능은 사용할 수 없습니다. 또한 보호 라이센스(subscription)의 경우 프로그램 데이터베이스가 업데이트되지 않고 컴퓨터 감시 및 검사 작업도 실행되지 않습니다.

어떠한 이유로 라이센스가 적시에 갱신되지 않은 경우(라이센스(subscription) 상태 – *업데이트 필요*), 예를 들어 라이센스 갱신이 가능한 시간 내내 컴퓨터가 꺼져 있었던 경우 상태를 직접 갱신할 수 있습니다. 라이센스(subscription) 갱신 시점까지 카스퍼스키 안티 바이러스는 라이센스(subscription)의 경우 프로그램 데이터베이스를 업데이트하지 않고 보호 라이센스(subscription)의 경우 컴퓨터 감시와 검사 작업을 일체 수행하지 않습니다.

라이센스(subscription)를 사용하는 경우 다른 활성화코드를 사용하여 라이센스를 갱신할 수 없습니다. 이 옵션은 라이센스(subscription)가 만료된(라이센스(subscription) 상태 – *만료됨*) 후에만 사용할 수 있습니다. 라이센스를 갱신할 수 있도록 유예 기간이 주어지며 이 기간 동안에는 프로그램의 기능이 유지됩니다.

라이센스(subscription)를 사용하여 컴퓨터에 프로그램을 다시 설치하는 경우 제품 구입 시 받은 활성화코드를 사용하여 직접 제품을 다시 활성화해야 합니다.

라이센스(subscription) 구매처에 따라 라이센스(subscription)에 대해 수행할 수 있는 처리 방법이 달라질 수 있습니다. 또한 라이센스 갱신이 가능한 유예 기간은 기본적으로 제공되지 않습니다.

카스퍼스키 시큐리티 네트워크 참가

전 세계적으로 날마다 수많은 신종 보안위협이 나타나고 있습니다. 카스퍼스키 랩은 신종 보안위협 및 경로에 대한 통계를 간편하게 수집하고 제거 방법을 신속히 개발할 수 있도록 카스퍼스키 시큐리티 네트워크 서비스를 사용할 것을 권장합니다.

카스퍼스키 시큐리티 네트워크를 사용하면 다음 정보가 카스퍼스키 랩에 전송됩니다:

- 카스퍼스키 안티 바이러스에서 사용자 컴퓨터에 할당한 고유 확인자. 컴퓨터의 하드웨어 설정을 파악하며 개인 정보는 포함하지 않습니다.
- 프로그램 구성요소에서 탐지한 보안위협에 대한 정보. 정보 구조 및 컨텐츠는 탐지되는 보안위협 형태에 따라 다릅니다.
- 시스템 정보: 운영 체제 버전, 설치된 서비스 팩, 다운로드되는 서비스 및 드라이버, 브라우저 및 메일 클라이언트 버전, 브라우저 확장자, 설치된 카스퍼스키 랩 프로그램의 버전 번호.

또한 카스퍼스키 시큐리티 네트워크는 다음 정보를 비롯한 폭넓은 통계를 수집합니다:

- 사용자 컴퓨터에 다운로드되는 실행 파일 및 서명이 들어 있는 프로그램;
- 사용자 컴퓨터에서 실행되는 프로그램.

통계 정보는 프로그램 업데이트가 완료되면 전송됩니다.

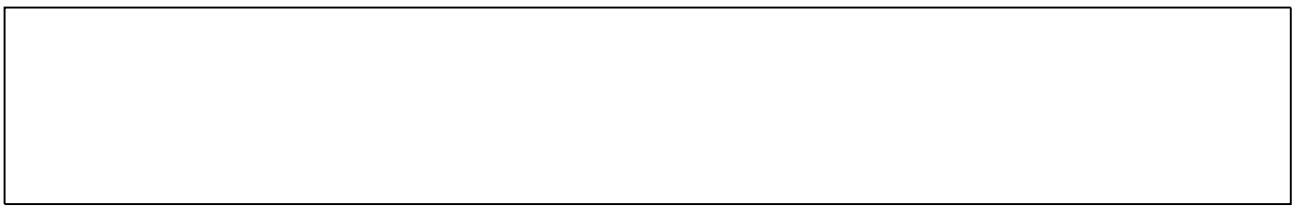
카스퍼스키 랩은 카스퍼스키 시큐리티 네트워크 내에서 사용자의 개인 정보를 수집하거나 배포하지 않는다는 것을 보장합니다.

- *통계 전송 설정을 구성하려면 다음과 같이 하십시오:*

1. 프로그램 설정 창을 엽니다.
2. 창 왼쪽에서 **정보 제공** 섹션을 선택합니다.
3. 카스퍼스키 시큐리티 네트워크에 참가한다는 것을 확인하려면 ☐ **[동의] 카스퍼스키 시큐리티 네트워크에 참가하겠습니다** 상자를 체크합니다.

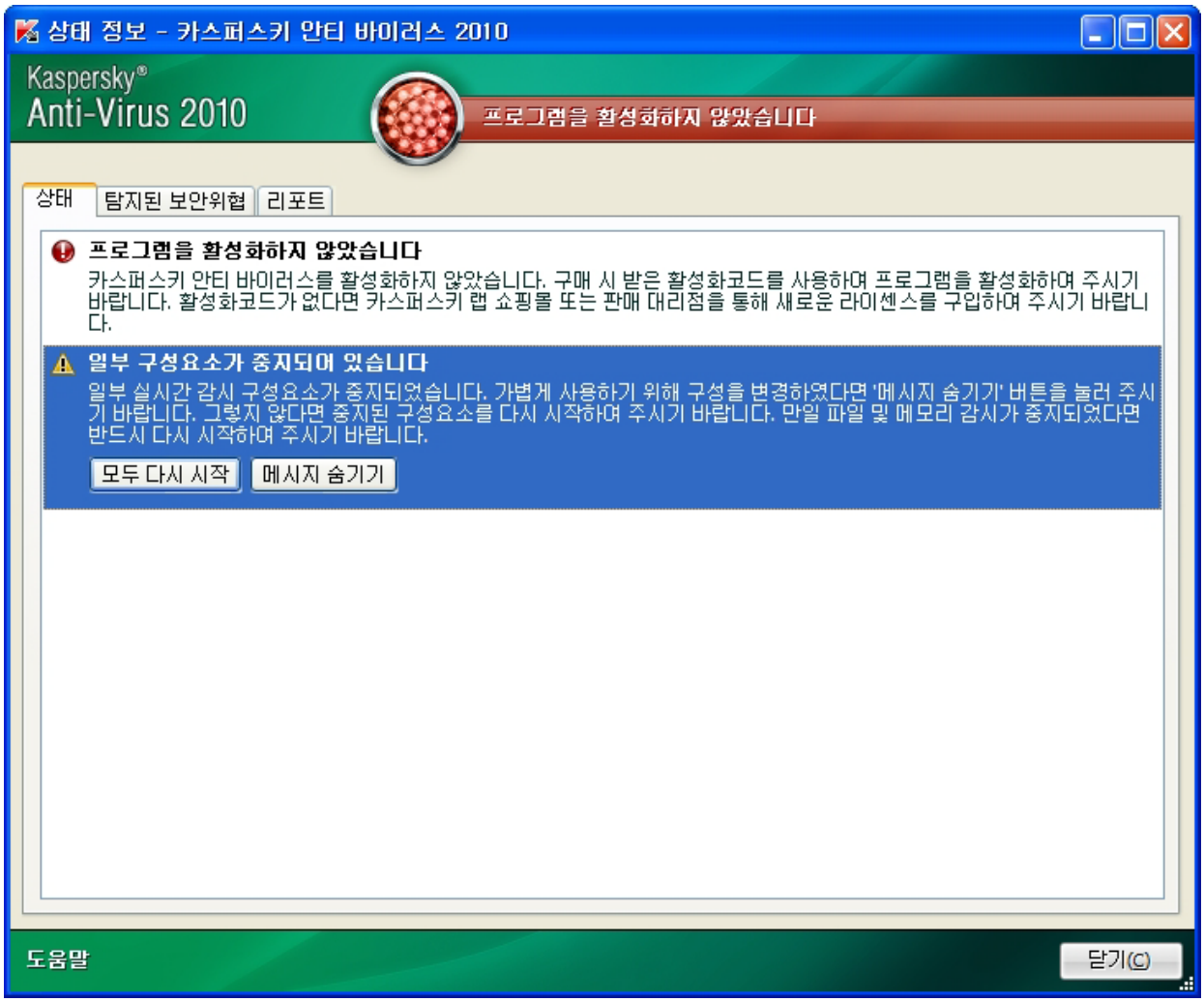
보안 관리

컴퓨터 감시에 문제가 발생할 경우 컴퓨터 감시 상태를 통해 알 수 있습니다. 감시 상태 아이콘과 아이콘이 위치한 패널의 색이 바뀝니다. 실시간 감시 시스템에 문제가 나타나면 즉시 수정할 것을 권장합니다.



현재 컴퓨터 감시 상태

발생한 문제 목록, 설명 및 가능한 해결 방법을 **상태** 탭에서 볼 수 있습니다(아래 그림 참조). 상태 아이콘 또는 아이콘이 있는 패널을 누르면 상태 탭을 선택할 수 있습니다.


상태 정보 - 카스퍼스키 안티 바이러스 2010
Kaspersky®
Anti-Virus 2010
프로그램을 활성화하지 않았습니다
상태
탐지된 보안위협
리포트
프로그램을 활성화하지 않았습니다
카스퍼스키 안티 바이러스를 활성화하지 않았습니다. 구매 시 받은 활성화코드를 사용하여 프로그램을 활성화하여 주시기 바랍니다. 활성화코드가 없다면 카스퍼스키 랩 쇼핑몰 또는 판매 대리점을 통해 새로운 라이센스를 구입하여 주시기 바랍니다.
일부 구성요소가 중지되어 있습니다
일부 실시간 감시 구성요소가 중지되었습니다. 가볍게 사용하기 위해 구성을 변경하였다면 '메시지 숨기기' 버튼을 눌러 주시기 바랍니다. 그렇지 않다면 중지된 구성요소를 다시 시작하여 주시기 바랍니다. 만일 파일 및 메모리 감시가 중지되었다면 반드시 다시 시작하여 주시기 바랍니다.
모두 다시 시작
메시지 숨기기
도움말
닫기(C)

보안 문제 해결

이 탭에는 현재 문제 목록이 표시됩니다. 문제는 위험도에 따라 정렬되어 있습니다. 가장 위험한 문제(빨강 아이콘), 덜 위험한 문제(노랑 아이콘) 순으로 표시되고 마지막에 정보 메시지가 표시됩니다. 각 문제에 대한 자세한 설명이 제공됩니다. 다음과 같은 처리 방법을 사용할 수 있습니다:

- *즉시 제거.* 해당 버튼을 사용하여 문제를 해결하도록 전환할 수 있습니다. 이것이 권장되는 처리 방법입니다.
- *제거 연기.* 어떠한 이유로 문제를 즉시 제거할 수 없는 경우 제거를 연기했다가 나중에 다시 돌아올 수 있습니다. 이렇게 하려면 **메시지 숨기기** 버튼을 누릅니다.

  이 옵션은 심각한 문제의 경우 사용할 수 없습니다. 심각한 문제로는 치료되지 않은 악성 개체, 하나 이상의 구성요소 장애, 프로그램 파일 손상 등이 포함됩니다.

숨긴 메시지를 일반 목록에 다시 표시하려면 ☐ **숨겨진 메시지 보이기** 상자를 체크합니다.

실시간 감시 상태

카스퍼스키 안티 바이러스 구성요소 성능 및 바이러스 검사 작업은 컴퓨터 감시 상태에 대한 요약 정보가 포함된 섹션에 기록됩니다. 여기서 카스퍼스키 안티 바이러스에서 탐지한 위험 및 감염의심 개체 수와 치료, 삭제 또는 격리된 개체를 파악할 수 있습니다.

컴퓨터 감시 상태는 카스퍼스키 안티 바이러스에서 탐지된 악성 개체에 대해 감시 상태 아이콘 및 아이콘이 위치한 패널의 색을 바꿈으로써 사용자에게 경고합니다. 악성 개체가 탐지될 경우 아이콘 및 패널의 색이 빨강으로 변합니다. 이 경우 출현하는 모든 보안위협을 즉시 제거해야 합니다.

- *컴퓨터 감시 상태에 대한 정보를 보는 방법은 다음과 같습니다:*

  1. 메인 프로그램 창을 엽니다.
  2. **리포트** 링크를 누릅니다.

- *컴퓨터 감시에서 발생한 문제를 제거하는 방법은 다음과 같습니다:*

  1. 메인 프로그램 창을 엽니다.
  2. **리포트** 링크를 누릅니다.
  3. 열리는 창의 상태 탭에서 필요한 작업을 수행합니다. 숨긴 메시지를 일반 목록에 다시 표시하려면 ☐ **숨겨진 메시지 보이기** 상자를 체크합니다.

- *탐지된 개체에 대해 처리 방법을 수행하는 방법은 다음과 같습니다:*

  1. 메인 프로그램 창을 엽니다.
  2. **리포트** 링크를 누릅니다.
  3. 열리는 창의 탐지된 보안위협 탭에 있는 개체 목록에서 필요한 개체를 선택하고 마우스 오른쪽 버튼을 누릅니다.
  4. 열리는 마우스 오른쪽 메뉴에서 필요한 작업을 선택합니다.

- *감시 구성요소 작동에 대한 리포트를 보는 방법은 다음과 같습니다:*

  1. 메인 프로그램 창을 엽니다.
  2. **리포트** 링크를 누릅니다.
  3. 열리는 창에서 리포트 탭을 선택합니다.

실시간 감시 일시 중지

실시간 감시를 일시 중지하면 일정 기간 동안 잠시 모든 실시간 감시 구성요소가 중지됩니다.

임시로 실시간 감시를 중지하면 모든 실시간 감시 구성요소가 일시 중지됩니다. 이는 다음을 통해 알 수 있습니다:

- 작업 표시줄 알림 영역의 프로그램 아이콘이 비활성(회색);
- 메인 프로그램 창의 상태 아이콘 및 패널이 빨강색.

네트워크 연결이 설정된 상태에서 실시간 감시를 일시 중지한 경우 연결이 종료되었다는 알림이 표시됩니다.

- *컴퓨터 감시를 일시 중지하려면 다음과 같이 하십시오:*

1. 프로그램의 마우스 오른쪽 메뉴에서 **실시간 감시 일시 중지** 항목을 선택합니다.
2. 열리는 **실시간 감시 일시 중지** 창에서 감시를 다시 시작할 시간 간격을 선택합니다:
   - **<시간 간격>후에 다시 시작 –** 지정한 시간이 지나면 실시간 감시가 작동됩니다. 드롭다운 메뉴를 사용하여 시간 간격 값을 선택합니다.
   - **재부팅 후 다시 시작 –** 프로그램이 다시 시작되거나 시스템이 다시 시작(시스템 시작 후 카스퍼스키 안티 바이러스가 자동으로 시작되도록 설정된 경우)된 후 실시간 감시가 작동됩니다.
   - **사용자가 직접 다시 시작** – 사용자가 직접 실시간 감시를 다시 시작해야 합니다. 실시간 감시를 작동하려면 프로그램의 마우스 오른쪽 메뉴에서 실시간 감시 다시 시작 항목을 선택합니다.

프로그램 인터페이스

카스퍼스키 안티 바이러스는 상당히 간단하고 편리한 인터페이스를 갖고 있습니다. 이 섹션에서는 이러한 인터페이스의 기본적인 기능을 자세히 설명합니다.

카스퍼스키 안티 바이러스에는 Microsoft Office Outlook(바이러스 검사 및 스팸 검사), The Bat! (바이러스 검사 및 스팸 검사), Microsoft Internet Explorer, Microsoft Windows Explorer 에 대한 플러그인이 포함되어 있습니다. 플러그인은 호스트 프로그램의 기능을 확장하여 해당 인터페이스에서 프로그램의 구성요소를 구성할 수 있도록 합니다.

참조:

알림 영역 아이콘 41

마우스 오른쪽 메뉴 42

카스퍼스키 안티 바이러스 메인 창 43

알림 46

프로그램 설정 창 46

알림 영역 아이콘

카스퍼스키 안티 바이러스를 설치하면 즉시 프로그램 아이콘이 Microsoft Windows 작업 표시줄 알림 영역에 나타납니다.

이 아이콘은 프로그램의 작동 상태를 알려줍니다. 또한 실시간 감시 상태와 프로그램에서 수행하는 몇 가지 기본적인 기능을 확인할 수 있습니다.

아이콘이 활성화 (컬러) 되면 실시간 감시가 완전히 작동되거나 일부 구성요소가 실행 중인 것입니다. 아이콘이 비활성화 (흑백) 되면 모든 실시간 감시 구성요소가 중지된 것입니다.

프로그램 아이콘은 수행되는 작동에 따라 변합니다:

– 이메일 검사 중입니다;

– 데이터베이스 및 프로그램 모듈 업데이트가 진행 중입니다;

– 업데이트를 적용하기 위해 컴퓨터를 재부팅해야 합니다;

– 일부 프로그램 구성요소 작동에 오류가 발생했습니다.

또한 프로그램 아이콘을 통해 프로그램 인터페이스의 기본 구성요소에 접근할 수 있습니다: 마우스 오른쪽 메뉴 및 메인 창.

프로그램 아이콘을 마우스 오른쪽 버튼으로 누르면 마우스 오른쪽 메뉴가 열립니다.

카스퍼스키 안티 바이러스 메인 창을 열려면 프로그램 아이콘을 마우스 왼쪽 버튼으로 누릅니다.

카스퍼스키 랩의 뉴스가 나온 경우 Microsoft Windows 작업 표시줄 알림 영역에 아이콘이 나타납니다. 해당 아이콘을 두 번 누르면 뉴스 텍스트가 열립니다.

마우스 오른쪽 메뉴

마우스 오른쪽 메뉴에서 기본적인 감시 작업을 실행할 수 있습니다,

카스퍼스키 안티 바이러스 마우스 오른쪽 메뉴에는 다음 항목이 포함되어 있습니다:

- **업데이트** – 프로그램 모듈 및 데이터베이스 업데이트를 시작하고 컴퓨터에 업데이트를 설치합니다.
- **컴퓨터 전체 검사** – 악성 개체가 있는지 확인하도록 컴퓨터에 대한 전체 검사를 시작합니다. 이동식 저장 장치를 비롯한 모든 드라이브에 있는 개체가 검사됩니다.
- **수동 검사** – 개체를 선택하고 바이러스 검사를 시작합니다. 기본적으로 목록에는 **내 문서** 폴더 및 사서함과 같은 여러 개체가 포함되어 있습니다. 목록을 확대하여 다른 검사 개체를 선택하여 바이러스 검사를 시작할 수 있습니다.
- **보안 키보드** – 보안 키보드로 전환합니다.
- **카스퍼스키 안티 바이러스 열기** – 메임 프로그램 창을 엽니다.
- **설정** – 프로그램 설정을 확인 및 구성합니다.
- **라이센스 등록** – 카스퍼스키 안티 바이러스 활성화 마법사로 이동합니다. 정식 사용자 자격을 얻으려면 프로그램을 활성화해야 합니다. 이 메뉴는 프로그램을 활성화하지 않은 경우만 사용할 수 있습니다.
- **프로그램 정보** – 프로그램에 대한 정보가 포함된 창을 표시합니다.
- **실시간 감시 일시 중지/실시간 감시 다시 시작** – 실시간 감시 구성요소를 일시적으로 중지 또는 작동합니다. 이 메뉴 옵션은 프로그램의 업데이트 또는 바이러스 검사 실행에 영향을 주지 않습니다.
- **종료** – 카스퍼스키 안티 바이러스를 종료합니다(이 옵션을 선택하면 프로그램이 컴퓨터 메모리에서 언로드됩니다).

마우스 오른쪽 메뉴

마우스 오른쪽 메뉴를 열 때 바이러스 검사 작업이 실행 중이면 해당 이름 및 진행 상태(완료율)가 마우스 오른쪽 메뉴에 표시됩니다. 해당 작업을 선택하면 현재 실행 결과에 대한 리포트가 포함된 메인 창으로 이동합니다.

카스퍼스키 안티 바이러스 메인 창

메인 프로그램 창은 세 부분으로 구분할 수 있습니다:

- 창 상단에는 현재 컴퓨터 감시 상태가 표시됩니다.

현재 컴퓨터 감시 상태

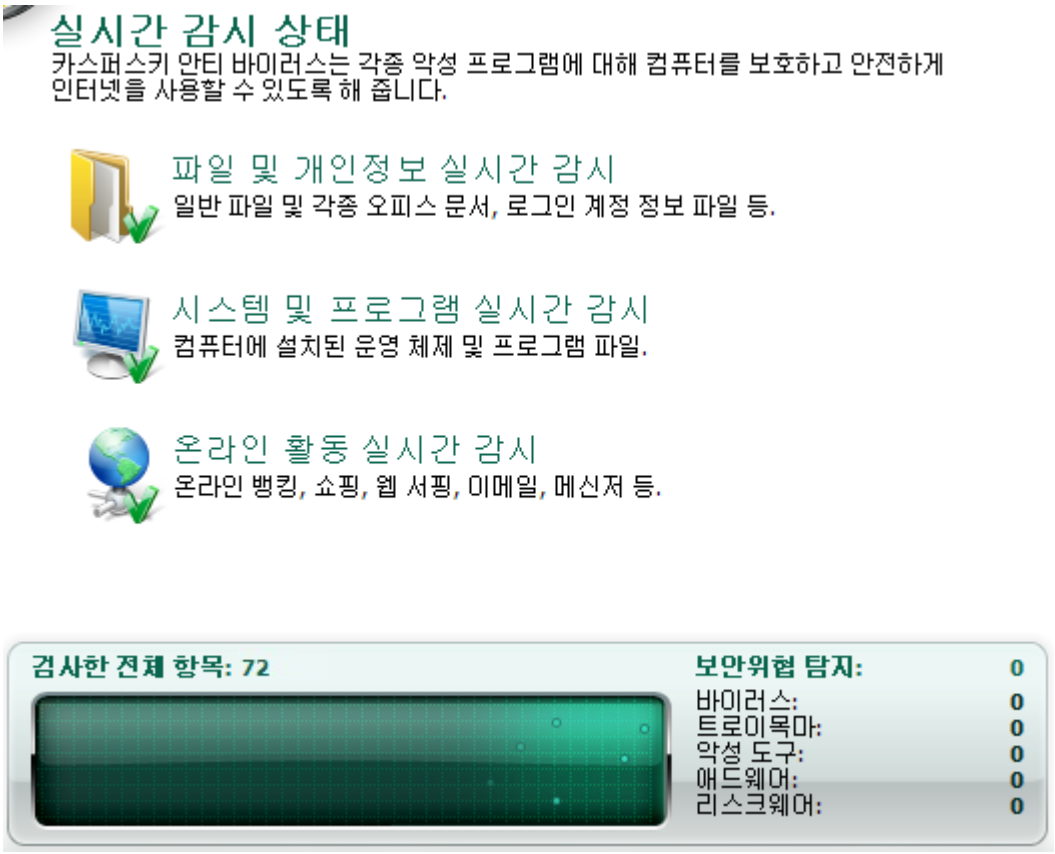
세 가지 가능한 감시 상태 값이 있습니다. 각 값은 교통 신호등과 비슷하게 특정 색으로 표시됩니다. 녹색은 컴퓨터 감시가 적절한 레벨로 이루어짐을 나타내고 노란색과 빨간색은 다양한 보안위협이 존재함을 나타냅니다. 보안위협에는 악성 프로그램 외에도 매우 오래된 프로그램 데이터베이스, 중지된 감시 구성요소, 최소 감시 설정 선택 등이 포함됩니다.

보안위협이 나타나면 제거해야 합니다. 보안위협과 이를 신속히 제거하는 방법에 대한 자세한 내용을 보려면 보안 관리 마법사로 이동하십시오. 상태 아이콘 및 아이콘이 위치한 패널(위 그림 참조)을 누르면 됩니다.

- 창 왼쪽 부분에서는 카스퍼스키 안티 바이러스의 모든 기능(바이러스 검사 작업, 업데이트 등)에 빠르게 접근할 수 있습니다.

메인 창 왼쪽

- 창 오른쪽 부분에는 왼쪽 부분에서 선택한 프로그램 기능에 대한 정보가 포함되어 있습니다. 여기서는 기능 설정을 구성하고 바이러스 검사 작업을 실행하는 도구와 업데이트를 검색하는 도구 등을 사용할 수 있습니다.


실시간 감시 상태
카스퍼스키 안티 바이러스는 각종 악성 프로그램에 대해 컴퓨터를 보호하고 안전하게 인터넷을 사용할 수 있도록 해 줍니다.
파일 및 개인정보 실시간 감시
일반 파일 및 각종 오피스 문서, 로그인 계정 정보 파일 등.
시스템 및 프로그램 실시간 감시
컴퓨터에 설치된 운영 체제 및 프로그램 파일.
온라인 활동 실시간 감시
온라인 뱅킹, 쇼핑, 웹 서핑, 이메일, 메신저 등.
검사한 전체 항목: 72
보안위협 탐지: 0
바이러스: 0
트로이목마: 0
악성 도구: 0
애드웨어: 0
리스크웨어: 0

메인 창 오른쪽

또한 다음 버튼 및 링크를 사용할 수 있습니다:

- **설정** – 카스퍼스키 안티 바이러스 설정 창을 엽니다.
- **격리 저장소** – 격리된 개체 작업을 시작합니다.
- **리포트** – 카스퍼스키 안티 바이러스 작동 중 발생한 이벤트 목록을 엽니다.
- **도움말** – 카스퍼스키 안티 바이러스 도움말 시스템을 봅니다.
- **내 카스퍼스키 계정** – 기술 지원 서비스를 받기 위해 홈페이지에 회원 가입을 할 수 있습니다.
- **지원** – 시스템에 대한 정보와 카스퍼스키 랩 정보 리소스에 대한 링크(기술 지원 서비스 사이트, 포럼)가 포함된 창을 엽니다.
- **라이센스** – 카스퍼스키 안티 바이러스 활성화, 라이센스 갱신.

다양한 그래픽 및 색상 구성표를 만들고 사용하여 카스퍼스키 안티 바이러스 인터페이스를 변경할 수 있습니다.

알림

카스퍼스키 안티 바이러스 작동 중 이벤트가 발생할 경우 Microsoft Windows 작업 표시줄의 프로그램 아이콘 위에 팝업 메시지로 특별한 알림이 표시됩니다.

이벤트가 컴퓨터 보안에 미치는 중요도에 따라 다음과 같은 유형의 알림이 표시됩니다:

- **경보**. 매우 중요한 이벤트가 발생했습니다. 예를 들어 시스템에서 바이러스 또는 위험한 활동이 탐지되었습니다. 해당 보안위협을 처리할 방법을 즉시 결정해야 합니다. 이 유형의 알림은 빨간색으로 표시됩니다.
- **경고**. 잠재적으로 위험할 수 있는 이벤트가 발생했습니다. 예를 들어 시스템에서 감염 위험이 있는 파일 또는 감염의심 활동이 탐지되었습니다. 해당 이벤트의 위험 정도를 확인해야 합니다. 이 유형의 알림은 노란색으로 표시됩니다.
- **정보**. 이 알림은 중요하지 않은 이벤트에 대한 정보를 제공합니다. 예를 들어 컨텐츠 필터링 구성요소 작동에 대한 알림을 제공합니다. 이 알림은 녹색으로 표시됩니다.

참조:

알림 148

프로그램 설정 창

카스퍼스키 안티 바이러스 설정 창은 메인 창 또는 마우스 오른쪽 메뉴를 통해 열 수 있습니다. 이 창을 열려면 메인 창 상단의 설정 링크를 누르거나 카스퍼스키 안티 바이러스의 마우스 오른쪽 메뉴에서 해당 옵션을 선택합니다.

프로그램 설정 창은 두 부분으로 구성됩니다:

- 창 왼쪽 부분에서는 카스퍼스키 안티 바이러스 기능, 수동 검사 작업, 업데이트 등에 접근할 수 있습니다.;
- 창 오른쪽 부분에는 창 왼쪽 부분에서 선택한 구성요소, 작업 등에 대한 설정 목록이 표시됩니다.

컴퓨터 파일 시스템 실시간 감시

*파일 안티 바이러스*는 컴퓨터 파일 시스템이 감염되지 않도록 보호합니다. 파일 안티 바이러스는 운영 체제를 시작할 때 로드되어 컴퓨터의 RAM 에서 실행되며 열려 있거나 저장되거나 실행되는 모든 파일을 검사합니다.

기본적으로 파일 안티 바이러스는 새 파일 또는 수정된 파일만 검사합니다. 보안 레벨이라는 설정 모음에 따라 파일 검사 방법이 결정됩니다. 파일 안티 바이러스가 보안위협을 탐지하면 지정된 처리 방법을 수행합니다.

사용 중인 컴퓨터의 파일 및 메모리 실시간 감시 레벨은 다음과 같은 설정 조합에 의해 결정됩니다:

- 실시간 감시 영역 생성 설정;
- 검사 형태 결정 설정;
- 복합 파일 검사 방법 결정 설정(대용량 복합 파일 검사 포함);
- 검사 모드 결정 설정;
- 스케줄 시작 또는 선택한 프로그램 작동 중에 구성요소를 일시 중지할 수 있는 설정.

카스퍼스키 랩의 전문가들은 파일 안티 바이러스 설정을 직접 구성하지 않을 것을 권장합니다. 대부분의 경우 보안 레벨을 변경하는 것만으로 충분합니다. 파일 안티 바이러스 기본 설정을 복원하려면 보안 레벨 중 하나를 선택하십시오.

- *파일 안티 바이러스 설정을 수정하려면 다음과 같이 하십시오:*

1. 메인 프로그램 창을 열고 창 상단의 **설정** 링크를 누릅니다.
2. 열리는 창의 **실시간 감시** 섹션에서 **파일 안티 바이러스** 구성요소를 선택합니다.
3. 선택한 구성요소의 **설정** 버튼을 누릅니다.
4. 구성요소 설정 중에서 필요한 사항을 변경합니다.

참조:

구성요소 연산 알고리즘 48

파일 및 메모리의 보안 레벨 변경 49

탐지된 개체에 수행할 처리 방법 변경 50

실시간 감시 영역 생성 50

휴리스틱 분석기 사용 51

감시 최적화 52

복합 파일 검사 52

대용량 복합 파일 검사 53

감시 방식 변경 54

고급 감시 기술 54

구성요소 일시 중지 스케줄 생성 55

구성요소 일시 중지 프로그램 목록 생성 56

기본 감시 설정 복원 57

구성요소 연산 알고리즘

운영 체제를 시작하면 *파일 안티 바이러스* 구성요소가 로딩되어 컴퓨터 메모리에서 실행되며 열려 있거나 저장 또는 실행되는 모든 파일을 검사합니다.

기본적으로 파일 안티 바이러스는 새로운 파일이나 변경된 파일, 즉 이전 검사 이후 추가 또는 변경된 파일만 검사합니다. 파일은 다음 알고리즘에 따라 검사됩니다:

1. 파일 안티 바이러스 구성요소가 사용자 및 프로그램의 모든 파일 접근 시도를 가로챕니다.

2. 파일 안티 바이러스 가 iChecker 및 iSwift 데이터베이스에서 가로챈 파일에 대한 정보를 검색하고 검색된 정보에 따라 해당 파일을 검사해야 할지 여부를 결정합니다.

검사 시 다음 작업이 수행됩니다:

1. 파일에서 바이러스를 검사합니다. 카스퍼스키 안티 바이러스 데이터베이스에 따라 악성 개체를 인지합니다. 데이터베이스에는 모든 악성 프로그램과 현재 알려진 보안위협, 그리고 이를 처리하는 방법에 대한 설명이 포함되어 있습니다.

2. 분석 후에 카스퍼스키 안티 바이러스에서 수행할 수 있는 처리 방법은 다음과 같습니다:

   a. 파일에서 악성 프로그램 코드가 탐지되는 경우 파일 안티 바이러스가 파일을 차단하고 백업 복사본을 만든 다음 치료를 수행합니다. 파일이 성공적으로 치료될 경우 다시 사용할 수 있습니다. 치료에 실패할 경우 파일이 삭제됩니다.

   b. 파일에서 잠재적으로 위험한 코드가 탐지될 경우(악성인지 확실치 않은 경우에도) 파일은 치료를 거쳐 격리 저장소라고 하는 특별한 저장 영역으로 전송됩니다.

   c. 파일에서 악성 코드가 발견되지 않은 경우 즉시 복원됩니다.

감염 또는 감염의심 파일이 탐지되는 경우 알림이 표시됩니다. 감염 또는 감염의심 개체가 탐지될 경우 추가 처리 방법이 필요하다는 알림이 화면에 표시됩니다. 다음과 같은 옵션이 주어집니다:

- 개체를 격리하여 이후에 업데이트된 데이터베이스를 사용하여 새로운 보안위협을 검사하고 처리합니다;
- 개체를 삭제합니다;
- 악성이 아니라고 확신하는 경우 개체를 건너뜁니다.

파일 및 메모리의 보안 레벨 변경

보안 레벨은 파일 안티 바이러스 구성요소 설정의 사전 설정 구성으로 정의됩니다. 카스퍼스키 랩 전문가는 세 가지 보안 레벨로 구분합니다. 사용자는 작동 조건 및 현재 상황을 토대로 레벨을 선택해야 합니다. 다음과 같은 보안 레벨 옵션 중 하나를 선택해야 합니다:

- **높음**. 컴퓨터가 감염될 위험이 매우 높다고 판단될 경우 이 레벨을 설정하십시오.
- **권장**. 이 레벨은 효율성과 보안을 최적으로 조합하여 대부분의 경우에 적합합니다.
- **낮음**. 보호된 환경(예: 중앙 집중식 보안 관리를 사용하는 기업 네트워크)에서 작업할 경우 낮은 보안 레벨이 적합할 수 있습니다. 또한 리소스 소모가 많은 프로그램으로 작업할 경우에도 낮은 보안 레벨로 설정할 수 있습니다.

낮은 보안 레벨을 사용하기 전에 높은 보안 레벨에서 컴퓨터를 전체적으로 검사하는 것이 좋습니다.

세 가지 사전 설정 레벨 중 적합한 레벨이 없다면 직접 파일 안티 바이러스 설정을 구성할 수 있습니다. 결과적으로 보안 레벨 이름은 **사용자 지정**으로 변경됩니다. 기본 구성요소 설정을 복원하려면 사전 설정된 보안 레벨 중 하나를 선택하십시오.

- *현재 파일 및 메모리 보안 레벨을 변경하려면 다음과 같이 하십시오:*

  1. 메인 프로그램 창을 열고 창 상단의 **설정** 링크를 누릅니다.
  2. 열리는 창의 **실시간 감시** 섹션에서 **파일 안티 바이러스** 구성요소를 선택합니다.

3. 선택한 구성요소에 필요한 보안 레벨을 설정합니다.

탐지된 개체에 수행할 처리 방법 변경

파일 안티 바이러스는 검사 결과를 기준으로 탐지된 개체에 다음 상태 중 하나를 적용합니다:

- 악성 프로그램(*바이러스* 또는 *트로이 목마* 등)
- *감염 위험 상태(검사 결과 개체가 감염되었는지 여부를 결정할 수 없는 경우).* 프로그램이 파일에서 알려지지 않은 바이러스의 코드 또는 알려진 바이러스의 변형된 코드를 탐지했음을 의미합니다.

카스퍼스키 안티 바이러스는 바이러스 검사 도중 감염 개체 또는 감염 위험 개체를 탐지한 경우 이를 사용자에게 알립니다. 사용자는 개체에 대한 처리 방법을 선택하여 보안위협에 대응해야 합니다. 카스퍼스키 안티 바이러스는 탐지된 개체에 대한 처리 방법으로 기본 설정인 **사용자 확인 후 처리** 옵션을 선택합니다. 처리 방법은 변경할 수 있습니다. 예를 들어, 탐지된 각 개체를 치료해야 하고 감염된 개체나 의심스러운 개체가 탐지되었다는 알림을 수신할 때마다 **치료** 처리 방법을 선택하지 않으려면 **사용자 확인 없이 치료**를 선택해야 합니다.

탐지된 개체를 치료하거나 삭제하기 전에 카스퍼스키 안티 바이러스는 이후 초기화 또는 치료를 허락하기 위해 개체의 백업 복사본을 생성합니다.

자동 모드에서 작업할 경우 위험 개체가 탐지되면 카스퍼스키 안티 바이러스가 카스퍼스키 랩의 전문가가 권장하는 처리 방법을 자동으로 적용합니다. 악성 개체의 경우 치료 방법은 **치료이고, 삭제해야 치료되는 것은 삭제**이며, 감염의심 개체의 경우 **건너뛰기**입니다.

- *탐지된 개체에 지정된 치료 방법을 변경하려면 다음과 같이 하십시오:*

  1. 메인 프로그램 창을 열고 창 상단의 **설정** 링크를 누릅니다.
  2. 열리는 창의 **실시간 감시** 섹션에서 **파일 안티 바이러스** 구성요소를 선택합니다.

  선택한 구성요소에 필요한 처리 방법을 지정합니다.

감시 영역 생성

감시 영역은 검사할 개체의 위치뿐 아니라 검사할 파일 형식을 의미합니다. 기본적으로 카스퍼스키 안티 바이러스는 하드 드라이브, 네트워크 드라이브 또는 이동식 장치에 저장된 감염 위험이 있는 파일만 검사합니다.

검사할 개체를 추가/제거하거나 검사할 파일 형식을 변경하여 감시 영역을 확장 또는 축소할 수 있습니다. 예를 들어 네트워크 드라이브에서 실행되는 exe 파일만 검사하기 원할 수 있습니다. 그러나 감시 영역을 축소함으로써 컴퓨터가 감염 위협에 노출되는 일이 없도록 주의해야 합니다.

파일 형식을 선택할 때는 다음 사항에 유의하십시오:

- 일부 파일 형식(예: *txt*)은 이후에 활성화될 수 있는 악성 코드를 포함할 위험이 낮습니다. 반면 실행 가능한 코드를 포함하거나 포함할 수 있는 파일 형식(*exe*, *dll*, *doc*)의 경우 악성 코드가 활성화될 위험이 상당히 높습니다.

- 그런데 침입자는 확장자가 *txt* 이지만 실행 파일로서 *txt* 로 이름만 변경한 파일을 통해 컴퓨터에 바이러스를 유포할 수 있습니다 **감염 가능성이 높은 파일 - 알려진 확장자** 옵션을 선택한 경우 그러한 파일의 검사를 건너뜁니다. 한편 **감염 가능성이 높은 파일 - 확장자 분석** 설정을 선택한 경우 확장자에 관계없이 파일 안티 바이러스에서 파일 헤더를 분석하여 파일이 실제로 *.exe* 파일이라는 점을 밝혀내고 바이러스를 검사합니다.

- *개체 검사 목록을 편집하려면 다음과 같이 하십시오:*

  1. 메인 프로그램 창을 열고 창 상단의 **설정** 링크를 누릅니다.
  2. 열리는 창의 **실시간 감시** 섹션에서 **파일 안티 바이러스** 구성요소를 선택합니다.
  3. 선택한 구성요소에서 **설정** 버튼을 누릅니다.
  4. 열리는 창의 **일반 설정** 탭, **감시 영역** 섹션에서 **추가** 링크를 누릅니다.
  5. **검사할 개체 선택** 창에서 개체를 선택하고 **추가** 버튼을 누릅니다.
  6. 필요한 모든 개체를 추가했으면 **검사할 개체 선택** 창에서 **확인** 버튼을 누릅니다.
  7. 검사 대상 개체 목록에서 개체를 제외시키려면 해당 개체 옆에 있는 상자를 체크해제합니다.

- *검사할 개체의 파일 형식을 변경하려면 다음과 같이 하십시오:*

  1. 메인 프로그램 창을 열고 창 상단의 **설정** 링크를 누릅니다.
  2. 열리는 창의 **실시간 감시** 섹션에서 **파일 안티 바이러스** 구성요소를 선택합니다.
  3. 선택한 구성요소에서 **설정** 버튼을 누릅니다.
  4. 열리는 창의 **일반 설정** 탭, **감시 파일 형태** 섹션에서 필요한 설정을 선택합니다.

휴리스틱 분석 사용

개체는 알려진 모든 악성 프로그램과 해당 치료 방법에 대한 설명이 포함된 데이터베이스를 사용하여 검사됩니다. 카스퍼스키 안티 바이러스는 각 검사 개체를 데이터베이스 레코드와 비교하여 악성 개체인지 여부와 악성 프로그램 종류(악성 개체일 경우)를 확인합니다. 이 방법은 *시그니처 분석*이라고 하며 기본적으로 항상 사용됩니다.

날마다 새로운 악성 프로그램 개체가 출현하기 때문에 데이터베이스에 설명되지 않은 악성 프로그램이 항상 있게 마련입니다. 이러한 악성 프로그램은 휴리스틱 분석을 사용해서만 탐지할 수 있습니다. 이 방법은 개체가 시스템 내에서 수행하는 활동을 분석하여 이루어집니다. 이러한 활동이 악성 개체에 일반적인 경우 개체는 악성 또는 감염의심으로 분류할 수 있습니다. 이를 통해 바이러스 애널리스트가 조사하기도 전에 새로운 보안위협을 탐지할 수 있습니다.

악성 개체가 탐지되는 경우 처리 방법을 수행하라는 알림이 표시됩니다.

또한 검사 레벨을 설정하여 새로운 보안위협 검색의 정밀도와 운영 체제 리소스의 로드, 검사에 소요되는 시간 간에 필요에 따라 균형을 맞출 수 있습니다. 분석 레벨이 높을수록 검사에 리소스가 많이 필요하고 시간이 오래 걸립니다.

- *휴리스틱 분석을 사용하고 검사 레벨을 설정하려면 다음과 같이 하십시오:*

  1. 메인 프로그램 창을 열고 창 상단의 **설정** 링크를 누릅니다.
  2. 열리는 창의 **실시간 감시** 섹션에서 **파일 안티 바이러스** 구성요소를 선택합니다.
  3. 선택한 구성요소에서 **설정** 버튼을 누릅니다.
  4. 열리는 창의 **성능 설정** 탭, **감시 방법** 섹션에서 ☑ **휴리스틱 분석** 상자를 체크하고 감시 레벨을 지정합니다.

검사 최적화

검사 시간을 단축하고 카스퍼스키 안티 바이러스 작동 속도를 높이도록 새로운 파일과 마지막 분석 후 변경된 파일만 검사하도록 선택할 수 있습니다. 이 모드는 단순 파일과 복합 파일 모두에 적용됩니다.

- *새로운 파일과 마지막 검사 후 변경된 파일만 검사하려면 다음과 같이 하십시오:*

  1. 메인 프로그램 창을 열고 창 상단의 **설정** 링크를 누릅니다.
  2. 열리는 창의 **실시간 감시** 섹션에서 **파일 안티 바이러스** 구성요소를 선택합니다.
  3. 선택한 구성요소에서 **설정** 버튼을 누릅니다.
  4. 열리는 창의 성능 설정 탭, 감시 최적화 섹션에서 ☑ **새로운 것이나 변경된 파일만 감시** 상자를 체크합니다.

복합 파일 검사

바이러스를 숨기는 데 흔히 사용되는 방법 한 가지는 압축 파일, 데이터베이스 등과 같은 복합 파일에 바이러스를 포함하는 것입니다. 이런 방식으로 숨겨진 바이러스를 탐지하려면 복합 파일을 압축해제해야 합니다. 이렇게 하면 검사 속도는 상당히 느려질 수 있습니다.

OLE 개체가 포함된 설치 패키지 및 파일은 열리는 동시에 실행되므로 압축 파일보다 더 위험합니다. 압축 파일 검사를 중지하고 이러한 파일 형식에 대한 검사를 작동하면 악성 코드 실행으로부터 컴퓨터를 보호하는 동시에 검사 속도를 높일 수 있습니다.

기본적으로 카스퍼스키 안티 바이러스는 포함된 OLE 개체만 검사합니다.

- *검사할 복합 파일 목록을 변경하려면 다음과 같이 하십시오:*

    1. 메인 프로그램 창을 열고 창 상단의 **설정** 링크를 누릅니다.
    2. 열리는 창의 **실시간 감시** 섹션에서 **파일 안티 바이러스** 구성요소를 선택합니다.
    3. 선택한 구성요소에서 **설정** 버튼을 누릅니다.
    4. 열리는 창의 **성능 설정** 탭, **복합 파일 검사** 섹션에서 카스퍼스키 안티 바이러스로 검사할 복합 파일 형식에 해당하는 상자를 체크 ☑ 합니다.

대용량 복합 파일 검사

대용량 복합 파일을 검사하는 경우 일차적인 압축해제만도 오랜 시간이 걸릴 수 있습니다. 백그라운드에서 파일을 검사할 경우 이 시간을 줄일 수 있습니다. 대용량 복합 파일 작업 시 악성 개체가 탐지될 경우 이에 대한 알림이 표시됩니다.

복합 파일 접근 시의 지연을 줄이도록 지정한 제한보다 큰 파일의 압축해제를 중지할 수 있습니다. 압축 파일에서 압축해제된 파일은 항상 검사됩니다.

- *카스퍼스키 안티 바이러스가 대용량 파일을 백그라운드에서 압축해제하도록 하려면 다음과 같이 하십시오:*

    1. 메인 프로그램 창을 열고 창 상단의 **설정** 링크를 누릅니다.
    2. 열리는 창의 **실시간 감시** 섹션에서 **파일 안티 바이러스** 구성요소를 선택합니다.
    3. 선택한 구성요소에서 **설정** 버튼을 누릅니다.
    4. 열리는 창의 **성능 설정** 탭, **복합 파일 검사** 섹션에서 **고급** 버튼을 누릅니다.
    5. **복합 파일** 창에서 ☑ **백그라운드에서 복합 파일 압축해제** 상자를 체크하고 아래 칸에 최소 파일 크기를 지정합니다.

- *카스퍼스키 안티 바이러스가 대용량 파일을 압축해제하지 않도록 하려면 다음과 같이 하십시오:*

    1. 메인 프로그램 창을 열고 창 상단의 **설정** 링크를 누릅니다.
    2. 열리는 창의 **실시간 감시** 섹션에서 **파일 안티 바이러스** 구성요소를 선택합니다.
    3. 선택한 구성요소에서 **설정** 버튼을 누릅니다.
    4. 열리는 창의 **성능 설정** 탭, **복합 파일 검사** 섹션에서 **고급** 버튼을 누릅니다.
    5. 열리는 **복합 파일** 창에서 ☑ **다음보다 큰 복합 파일은 압축해제 안함** 상자를 체크하고 옆에 있는 칸에서 파일 크기를 지정합니다.

감시 방식 변경

감시 방식은 파일 안티 바이러스를 작동시키는 조건입니다. 카스퍼스키 안티 바이러스의 기본 설정은 스마트 모드입니다. 즉, 개체에 수행되는 작업에 따라 개체 검사 여부를 결정합니다. 예를 들어 Microsoft Office 문서 작업의 경우 카스퍼스키 안티 바이러스는 파일이 처음 열릴 때와 마지막에 닫힐 때 파일을 검사합니다. 그 사이에 파일에 쓰는 작업은 검사되지 않습니다.

개체 감시 방식을 변경할 수 있습니다. 감시 방식은 주로 작업하는 파일 유형에 따라 선택해야 합니다.

- *개체 감시 방식을 변경하려면 다음과 같이 하십시오:*

  1. 메인 프로그램 창을 열고 창 상단의 **설정** 링크를 누릅니다.
  2. 열리는 창의 **실시간 감시** 섹션에서 **파일 안티 바이러스** 구성요소를 선택합니다.
  3. 선택한 구성요소에서 **설정** 버튼을 누릅니다.
  4. 열리는 창의 **고급 설정** 탭, **감시 방식** 섹션에서 필요한 모드를 선택합니다.

고급 감시 기술

또한 파일 안티 바이러스 구성요소에서 사용할 기술을 지정할 수 있습니다:

- **iChecker**. 이 기술은 검사에서 일부 개체를 제외하여 검사 속도를 높여 줍니다. 개체는 카스퍼스키 안티 바이러스 데이터베이스 배포 날짜, 마지막 개체 검사 날짜, 스캔 설정 변경 사항 등을 고려하는 특별 알고리즘을 사용하여 검사에서 제외됩니다.

  예를 들어 압축 파일 검사 후 *감염되지 않음* 상태가 할당되었다고 해봅시다. 이 압축 파일이 바뀌거나 검사 설정이 변경되지 않은 경우 프로그램은 다음 번에 이 압축 파일을 검사에서 제외합니다. 새 개체가 추가되어 압축 파일 구조가 바뀌었거나 검사 설정이 변경되었거나 프로그램 데이터베이스가 업데이트된 경우에는 압축 파일이 다시 검사됩니다.

  iChecker 에는 몇 가지 제한이 있습니다. 대용량 파일에는 작동할 수 없고 카스퍼스키 안티 바이러스에서 인지하는 구조(예: *.exe*, *.dll*, *.lnk*, *.ttf*, *.inf*, *.sys*, *.com*, *.chm*, *.zip*, *.rar*)를 가진 개체에만 적용됩니다.

- **iSwift**. 이 기술은 iChecker 기술을 NTFS 파일 시스템을 사용하는 컴퓨터에 사용하도록 발전시킨 것입니다. iSwift 에는 몇 가지 제한이 있습니다. 파일 시스템의 특정 파일 위치에만 해당되므로 NTFS 에 있는 개체에만 적용할 수 있습니다.

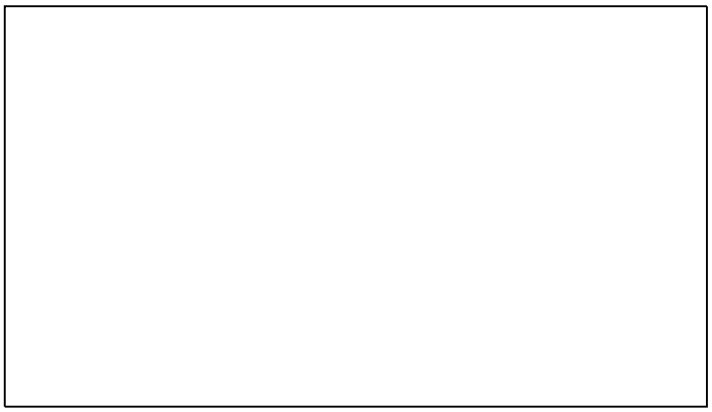
- *개체 감시 기술을 변경하려면 다음과 같이 하십시오:*

  1. 메인 프로그램 창을 열고 창 상단의 **설정** 링크를 누릅니다.
  2. 열리는 창의 **실시간 감시** 섹션에서 **파일 안티 바이러스** 구성요소를 선택합니다.
  3. 선택한 구성요소에서 **설정** 버튼을 누릅니다.

4. 열리는 창의 **고급 설정** 탭, **고급 감시 기술** 섹션에서 필요한 설정 값을 선택합니다.

구성요소 일시 중지: 스케줄 생성

상당한 컴퓨터 리소스가 필요한 일부 프로그램 사용 중 개체에 보다 빠르게 접근하기 위해 파일 안티 바이러스 구성요소 작업을 일시 중지할 수 있습니다. 로드를 줄여 개체에 빠르게 접근하기 위해 파일 안티 바이러스 구성요소 작업을 중지할 스케줄을 설정할 수 있습니다.



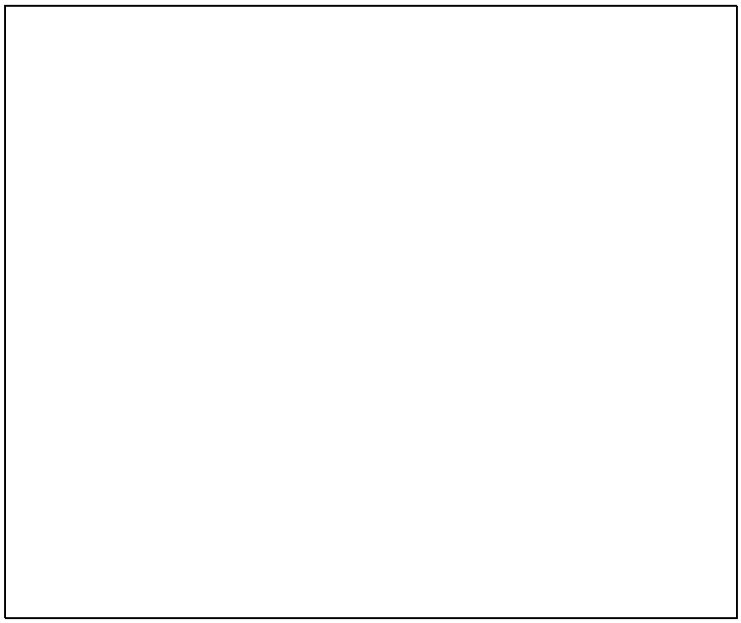
스케줄 생성

- *구성요소를 일시 중지할 스케줄을 구성하려면 다음과 같이 하십시오:*

  1. 메인 프로그램 창을 열고 창 상단의 **설정** 링크를 누릅니다.
  2. 열리는 창의 **실시간 감시** 섹션에서 **파일 안티 바이러스** 구성요소를 선택합니다.
  3. 선택한 구성요소에서 **설정** 버튼을 누릅니다.
  4. 열리는 창의 **고급 설정** 탭, **작업 일시 중지** 섹션에서 **스케줄에 따라 상자를 체크하고 설정 버튼을 누릅니다**.
  5. **작업 일시 중지** 창에서 실시간 감시를 일시 중지할 시간(24 시간 HH:MM 형식)을 지정합니다. (**작업 일시 중지 시간** 및 **작업 다시 시작 시간** 칸).

구성요소 일시 중지: 프로그램 목록 생성

상당한 컴퓨터 리소스가 필요한 일부 프로그램 사용 중 개체에 보다 빠르게 접근하기 위해 파일 안티 바이러스 구성요소 작업을 일시 중지할 수 있습니다. 로드를 줄여 개체에 빠르게 접근하기 위해 파일 안티 바이러스 구성요소 작업을 중지할 스케줄을 설정할 수 있습니다.



프로그램 목록 생성

파일 안티 바이러스 구성요소가 일부 프로그램과 충돌하는 경우 긴급 조치로 파일 안티 바이러스 구성요소를 중지하도록 구성할 수 있습니다. 파일 안티 바이러스 구성요소 작업 시 충돌이 발생하는 경우 카스퍼스키 랩 기술 지원 서비스(http://www.kaspersky.co.kr/service.html)에 문의하십시오. 지원 전문가가 컴퓨터에서 카스퍼스키 안티 바이러스와 해당 소프트웨어를 동시에 실행할 때의 문제를 해결할 수 있도록 도와 드립니다.

- *특정 프로그램 사용 중 파일 안티 바이러스 구성요소를 일시 중지하도록 구성하려면 다음과 같이 하십시오.*

1. 메인 프로그램 창을 열고 창 상단의 **설정** 링크를 누릅니다.
2. 열리는 창의 **실시간 감시** 섹션에서 **파일 안티 바이러스** 구성요소를 선택합니다.
3. 선택한 구성요소에서 **설정** 버튼을 누릅니다.
4. 열리는 창의 **고급 설정** 탭, **작업 일시 중지** 섹션에서 ☑ **프로그램 시작 시** 상자를 체크하고 **선택** 버튼을 누릅니다.
5. **프로그램** 창에서 실행 중 파일 안티 바이러스 구성요소를 일시 중지할 프로그램 목록을 생성합니다.

기본 감시 설정 복원

파일 안티 바이러스를 구성할 때 항상 권장 설정을 복원할 수 있습니다. 카스퍼스키 랩에서 최적의 설정으로 권장하며 **권장 보안** 레벨로 분류됩니다.

- *기본 감시 설정을 복원하려면 다음과 같이 하십시오:*

  1. 메인 프로그램 창을 열고 창 상단의 **설정** 링크를 누릅니다.
  2. 열리는 창의 실시간 **감시** 섹션에서 **파일 안티 바이러스** 구성요소를 선택합니다.
  3. **보안 레벨** 섹션에서 선택한 구성요소에 대해 **기본값** 버튼을 누릅니다.

메일 실시간 감시

메일 안티 바이러스는 보내고 받는 메시지에 악성 개체가 있는지 검사합니다. 메일 안티 바이러스는 운영 체제를 로드할 때 실행되며 컴퓨터의 RAM 에 위치하여 POP3, SMTP, IMAP, MAPI 및 NNTP 프로토콜을 통해 받는 모든 이메일 메시지를 검사합니다.

보안 레벨이라는 설정 모음에 따라 이메일 검사 방법이 결정됩니다. 보안위협이 탐지되면 메일 안티 바이러스가 지정한 처리 방법을 수행합니다. 이메일이 검사되는 규칙은 설정 모음에 의해 정의됩니다. 이러한 규칙은 그룹으로 분류되어 다음과 같은 기능을 결정할 수 있습니다:

- 보호된 메일 스트림에서;
- 휴리스틱 분석기 사용;
- 복합 파일 검사;
- 첨부된 파일 필터링.

카스퍼스키 랩은 메일 안티 바이러스 설정을 직접 구성하지 않을 것을 권장합니다. 대부분의 경우 다른 보안 레벨을 선택하는 것만으로 충분합니다. 메일 안티 바이러스 기본 설정을 복원할 수 있습니다. 이렇게 하려면 보안 레벨 중 하나를 선택하십시오.

- *메일 안티 바이러스 설정을 편집하려면 다음과 같이 하십시오:*

1. 메인 프로그램 창을 열고 창 상단의 **설정** 링크를 누릅니다.
2. 열리는 창의 **실시간 감시** 섹션에서 **메일 안티 바이러스** 구성요소를 선택합니다.
3. 선택한 구성요소의 **설정** 버튼을 누릅니다.
4. 구성요소 설정 중에서 필요한 사항을 변경합니다.

참조:

구성요소 연산 알고리즘 59

이메일 실시간 감시 보안 레벨 변경 60

탐지된 개체에 수행할 처리 방법 변경 61

실시간 감시 영역 생성 62

Microsoft Office Outlook 의 이메일 검사 62

The Bat!의 이메일 검사 63

휴리스틱 분석기 사용 64

복합 파일 검사 64

첨부파일 필터링 64

기본 메일 실시간 감시 설정 복원 65

구성요소 연산 알고리즘

카스퍼스키 안티 바이러스에는 이메일에서 위험한 개체를 검사하는 메일 안티 바이러스라는 구성요소가 포함되어 있습니다. 메일 안티 바이러스는 운영 체제 시작 시 로딩되어 지속적으로 실행되면서 POP3, SMTP, IMAP, MAPI 및 NNTP 프로토콜을 통한 이메일과 POP3 및 IMAP 을 통한 SSL 보안 접속 이메일을 모두 검사합니다.

메일 안티 바이러스 구성요소의 작동은 작업 표시줄 알림 영역의 프로그램 아이콘(□)으로 확인할 수 있습니다. 이메일 메시지를 검사할 때마다 이 아이콘이 표시됩니다.

기본적으로 이메일 감시는 다음과 같이 수행됩니다.

1. 사용자가 보내거나 받은 모든 이메일을 메일 안티 바이러스 구성요소에서 가로챕니다.
2. 이메일을 각 부분, 즉 이메일 제목, 본문, 첨부 파일로 나눕니다.
3. 이메일 메시지 본문과 첨부 파일(OLE 개체 포함)에서 위험 개체가 있는지 검사합니다. 악성 개체는 카스퍼스키 안티 바이러스 데이터베이스와 휴리스틱 알고리즘을 사용하여 탐지됩니다. 데이터베이스에는 현재까지 알려진 모든 악성 프로그램에 대한 설명과 이를 처리하는 방법이 포함되어 있습니다. 휴리스틱 알고리즘을 통해 데이터베이스에 아직 입력되지 않은 신종 바이러스를 탐지할 수 있습니다.
4. 바이러스 검사 후에는 다음과 같은 행동 옵션을 사용할 수 있습니다:

- 이메일 본문 또는 첨부 파일에 악성 코드가 포함된 경우 파일 안티 바이러스 구성요소는 해당 이메일을 차단하고 백업 복사본을 만든 다음 치료를 시도합니다. 성공적으로 치료된 이메일 메시지는 사용자에게 다시 돌아옵니다. 치료에 실패할 경우 감염 개체가 메시지에서 삭제됩니다. 바이러스 검사 후에는 이메일이 카스퍼스키 안티 바이러스에서 처리되었음을 알리는 특별한 텍스트가 이메일 제목 줄에 삽입됩니다.

- 본문 또는 첨부 파일에서 잠재적으로 위험한 코드가 탐지될 경우(악성인지 확실치 않은 경우에도) 해당 부분이 격리 저장소라고 하는 특별 저장 영역에 배치됩니다.

- 이메일에서 악성 코드가 발견되지 않은 경우 즉시 사용할 수 있는 상태로 복귀됩니다.

Microsoft Office Outlook 의 경우 특별한 플러그인이 제공됩니다. 이 플러그인을 통해 이메일 검사를 보다 정확하게 구성할 수 있습니다.

The Bat!을 사용하는 경우 카스퍼스키 안티 바이러스를 다른 안티 바이러스 프로그램과 함께 사용할 수 있습니다. 그 경우 이메일 트래픽 처리 규칙이 The Bat!에서 직접 구성되며 이 규칙이 카스퍼스키 안티 바이러스의 메일 감시 설정보다 우선합니다.

Microsoft Outlook Express/Windows Mail, Mozilla Thunderbird, Eudora, Incredimail 등과 같은 다른 메일 프로그램을 사용할 경우 메일 안티 바이러스 구성요소는 SMTP, POP3, IMAP 및 NNTP 프로토콜을 통한 이메일을 검사합니다.

Thunderbird 메일 클라이언트를 사용할 경우 **사서함** 폴더에서 메시지를 이동하는 필터를 사용하면 IMAP를 통해 전송되는 이메일 메시지에 대해 바이러스가 검사되지 않습니다.

이메일 실시간 감시 보안 레벨 변경

보안 레벨은 파일 안티 바이러스 설정의 사전 설정 구성으로 정의됩니다. 카스퍼스키 랩 전문가는 세 가지 보안 레벨로 구분합니다. 사용자는 작동 조건 및 현재 상황을 토대로 레벨을 선택해야 합니다. 다음 보안 레벨 중 하나를 선택할 수 있습니다:

- **높음.** 이 레벨은 보내고 받는 메시지 스트림을 가장 완벽하게 제어합니다. 메일 안티 바이러스가 첨부된 압축 파일을 용량에 관계 없이 검사합니다. 검사 강도가 가장 높은 레벨에서 휴리스틱 분석기가 실행됩니다.

- **권장.** 속도와 보안을 최적으로 조합한 레벨입니다. 메일 안티 바이러스가 보내고 받는 메시지 및 첨부된 압축 파일을 용량에 관계 없이 모두 검사합니다. 검사 강도가 가장 높은 레벨에서 휴리스틱 분석기가 실행됩니다.

- **낮음.** 이 레벨을 선택하면 가장 빠른 속도로 이메일을 검사할 수 있습니다. 메일 안티 바이러스가 받는 메시지만 검사하고 압축된 첨부파일은 검사하지 않습니다. 검사 강도가 가장 낮은 레벨에서 휴리스틱 분석기가 실행됩니다.

세 가지 사전 설정 레벨 중 적합한 레벨이 없다면 직접 메일 안티 바이러스 설정을 구성할 수 있습니다. 결과적으로 보안 레벨 이름은 사용자지정으로 변경됩니다. 기본 구성요소 설정을 복원하려면 사전 설정된 보안 레벨 중 하나를 선택하십시오.

- *사전 설정 이메일 보안 레벨을 변경하려면 다음과 같이 하십시오.:*

  1. 메인 프로그램 창을 열고 창 상단의 **설정** 링크를 누릅니다.
  2. 열리는 창의 **실시간 감시** 섹션에서 **메일 안티 바이러스** 구성요소를 선택합니다.
  3. 선택한 구성요소에 필요한 보안 레벨을 설정합니다.

탐지된 개체에 수행할 처리 방법 변경

메일 안티 바이러스는 이메일 메시지를 검사합니다. 검사 결과 이메일 또는 이메일의 일부분(본문, 첨부파일)이 감염되었거나 감염 위험이 있다고 나타날 경우 구성요소가 개체의 상태와 선택한 처리 방법에 따라 후속 조치를 결정합니다.

메일 안티 바이러스는 탐지된 개체에 다음 상태 중 하나를 검사 결과로 적용합니다:

- 악성 프로그램(바이러스 또는 트로이 목마 등);
- *감염 위험 상태(검사 결과 개체가 감염되었는지 여부를 결정할 수 없는 경우). 이메일 또는 첨부파일에 알려지지 않은 바이러스의 코드나 알려진 바이러스의 변형된 코드가 포함되어 있음을 의미합니다.*

카스퍼스키 안티 바이러스는 이메일 검사 도중 감염 개체 또는 감염 위험 개체를 탐지한 경우 이를 사용자에게 알립니다. 사용자는 **개체에 대한 처리 방법**을 선택하여 보안위협에 대응해야 합니다. 카스퍼스키 안티 바이러스는 탐지된 개체에 대한 처리 방법으로 기본 설정인 **사용자 확인 후 처리** 옵션을 선택합니다. 처리 방법은 변경할 수 있습니다. 예를 들어, 탐지된 각 개체를 치료해야 하고 메시지에서 감염된 개체나 의심스러운 개체가 탐지되었다는 알림을 수신할 때마다 치료 처리 방법을 선택하지 않으려면 **사용자 확인 없이 치료**를 선택해야 합니다

탐지된 개체를 치료하거나 삭제하기 전에 카스퍼스키 안티 바이러스는 이후 초기화 또는 치료를 허락하기 위해 개체의 백업 복사본을 생성합니다.

자동 모드에서 작업할 경우 위험 개체가 탐지되면 카스퍼스키 안티 바이러스는 카스퍼스키 랩의 전문가가 권장하는 처리 방법을 자동으로 적용합니다. 악성 개체의 경우 치료 방법은 치료이고, 삭제해야 치료되는 것은 **삭제**이며, 감염의심 개체의 경우 **건너뛰기**입니다.

- *탐지된 개체에 지정된 치료 방법을 변경하려면 다음과 같이 하십시오:*

  1. 메인 프로그램 창을 열고 창 상단의 **설정** 링크를 누릅니다.
  2. 열리는 창의 실시간 감시 섹션에서 메일 안티 바이러스 구성요소를 선택합니다.
  3. 선택한 구성요소에 필요한 처리 방법을 지정합니다.

실시간 감시 영역 생성

실시간 감시 영역은 검사되는 메시지의 형태를 말합니다. 기본적으로 카스퍼스키 안티 바이러스는 보내거나 받는 모든 이메일을 검사합니다. 받는 이메일만 검사하도록 설정하면 컴퓨터에 웜이 있을 경우 이메일을 통해 배포되므로 시작할 때 카스퍼스키 안티 바이러스를 사용하여 보내는 이메일을 검사하는 것이 좋습니다. 이렇게 하면 컴퓨터에서 감염된 이메일이 감시되지 않고 대량으로 발송됨으로 인해 발생하는 불쾌한 상황을 피할 수 있습니다.

실시간 감시 영역에는 또한 메일 안티 바이러스 구성요소를 시스템에 통합하는 데 사용되는 설정과 검사되는 프로토콜이 포함됩니다. 기본적으로 메일 안티 바이러스 구성요소는 Microsoft Office Outlook 과 The Bat! 이메일 클라이언트 프로그램에 통합됩니다.

- *보내는 이메일의 검사를 중지하려면 다음과 같이 하십시오:*

  1. 메인 프로그램 창을 열고 창 상단의 **설정** 링크를 누릅니다.
  2. 열리는 창의 **실시간 감시** 섹션에서 **메일 안티 바이러스** 구성요소를 선택합니다.
  3. 선택한 구성요소의 **설정** 버튼을 누릅니다.
  4. 열리는 창의 **일반** 설정 탭 아래 있는 **실시간 감시 영역** 섹션에서 원하는 설정 값을 선택합니다.

- *검사할 프로토콜과 메일 안티 바이러스를 시스템에 통합하는 데 필요한 설정을 선택하려면 다음과 같이 하십시오.*

  1. 메인 프로그램 창을 열고 창 상단의 **설정** 링크를 누릅니다.
  2. 열리는 창의 **실시간 감시** 섹션에서 **메일 안티 바이러스** 구성요소를 선택합니다.
  3. 선택한 구성요소의 설정 버튼을 누릅니다.
  4. 열리는 창의 고급 설정 탭 아래 있는 연결 섹션에서 필요한 설정을 선택합니다.

MICROSOFT OFFICE OUTLOOK 의 이메일 검사

Microsoft Office Outlook 을 이메일 클라이언트로 사용하는 경우 메일의 바이러스 검사를 수행하기 위한 추가 설정을 구성할 수 있습니다.

카스퍼스키 안티 바이러스를 설치할 때 특수 플러그인이 Microsoft Office Outlook 에 설치됩니다, 메일 안티 바이러스 설정을 빠르게 구성할 수 있고 이메일 메시지가 위험 개체인지 검사하는 시간을 결정할 수 있습니다.

플러그인은 도구 → 옵션 메뉴에 있는 특수 이메일 감시 탭의 형태로 제공됩니다. 탭에서 다음과 같은 이메일 검사 모드를 지정할 수 있습니다.

- *상세한 필터링 조건을 지정하려면 다음과 같이 하십시오:*

  1. 메인 Microsoft Outlook 프로그램 창을 엽니다.

2. 프로그램 메뉴에서 **도구 → 옵션**을 선택합니다.

3. **이메일 감시** 탭에서 필요한 이메일 검사 모드를 지정합니다.

The Bat!의 이메일 검사

The Bat!의 감염된 이메일 개체에 취해진 조치는 프로그램 자체 도구를 사용하여 정의됩니다.

보내고 받는 메시지를 검사할지 여부, 이메일의 위험 개체에 수행할 처리, 적용할 제외 규칙 등을 결정하는 메일 안티 바이러스 설정은 무시됩니다. The Bat!에서는 첨부된 압축 파일을 검사할지 여부만 고려합니다.

이메일 감시 설정은 the Bat!를 지원하는 컴퓨터에 설치되어 있는 모든 안티 바이러스 모듈로 확장됩니다.

보내고 받는 메시지는 먼저 메일 안티 바이러스로 검사한 후에만 The Bat! 메일 클라이언트 플러그인으로 검사합니다. 악성 개체가 탐지될 경우 카스퍼스키 안티 바이러스는 반드시 이 사실을 사용자에게 알립니다. 메일 안티 바이러스의 알림 창에서 **치료(삭제) 처리**를 선택한 경우 메일 안티 바이러스에서는 보안위협을 제거할 목적으로 처리를 수행합니다. 알림 창에서 **건너뛰기** 처리를 선택한 경우 The Bat! 플러그인에서 개체를 치료합니다. 이메일 메시지를 보낼 때 플러그인에서 먼저 검사를 수행한 다음 메일 안티 바이러스에서 검사를 수행합니다.

사용자는 다음 사항을 결정해야 합니다.

- 검사할 이메일 메시지의 스트림(보내거나 받는 메시지)
- 이메일 개체의 검사를 수행할 시간(이메일 메시지를 열 때 또는 이메일 메시지를 디스크에 저장하기 전)
- 이메일에서 위험 개체가 탐지되는 경우 메일 클라이언트에서 수행할 처리. 예를 들어 다음을 선택할 수 있습니다.
    - **감염된 부분의 치료 시도** - 이 옵션을 선택한 경우 감염된 개체의 치료를 시도하고 치료할 수 없는 경우 해당 개체는 메시지에 그대로 남습니다.
    - **감염된 부분 삭제** - 이 옵션을 선택한 경우 감염 여부 또는 감염 의심 여부에 상관 없이 메시지의 위험 개체를 삭제합니다.

기본적으로 The Bat!는 감염된 모든 이메일 개체를 치료하려고 시도하지 않고 격리저장소에 둡니다.

The Bat!는 위험 개체를 포함하고 있는 이메일에 특수한 헤더를 지정하지 않습니다.

- *The Bat!에서 이메일 감시 규칙을 설정하려면 다음과 같이 하십시오.*

1. The Bat! 메인 창을 엽니다.

2. 메일 클라이언트의 **속성** 메뉴에서 **설정** 항목을 선택합니다.

3. 설정 트리에서 **바이러스 감시** 항목을 선택합니다.

휴리스틱 분석기 사용

기본적으로 휴리스틱 방법은 시스템에서의 개체 활동을 분석합니다. 이러한 활동이 악성 개체에 일반적인 경우 개체는 악성 또는 감염의심으로 분류할 수 있습니다. 이 방법을 사용하면 새로운 보안위협을 바이러스 애널리스트에서 분석하기 전에 미리 탐지할 수 있습니다. 기본적으로 휴리스틱 분석기가 작동합니다.

카스퍼스키 안티 바이러스는 이메일에서 탐지된 악성 개체를 사용자에게 알립니다. 알림에 반응하여 메시지를 처리해야 합니다.

또한 검사 레벨을 **기본, 자세히, 매우 자세히** 등 상세하게 설정할 수 있습니다. 이렇게 하려면 슬라이더 막대를 선택한 위치로 옮겨야 합니다.

- *휴리스틱 분석기를 작동/중지하고 검사 레벨을 설정하려면 다음과 같이 하십시오:*

  1. 메인 프로그램 창을 열고 창 상단의 **설정** 링크를 누릅니다.
  2. 열리는 창의 실시간 **감시** 섹션에서 **메일 안티 바이러스** 구성요소를 선택합니다.
  3. 선택한 구성요소의 **설정** 버튼을 누릅니다.
  4. 열리는 창의 **일반** 설정 탭 아래 있는 **감시 방법** 섹션에서 ☐ **휴리스틱 분석기** 상자를 체크/체크해제하고 검사 상세 레벨을 지정합니다.

복합 파일 검사

복합 파일 감시 방식를 선택하면 카스퍼스키 안티 바이러스 성능이 영향을 받습니다. 첨부된 압축 파일의 검사를 작동하거나 중지하고 검사되는 압축 파일의 최대 크기를 제한할 수 있습니다.

- *복합 파일 검사를 위한 설정을 구성하려면 다음과 같이 하십시오:*

  1. 메인 프로그램 창을 열고 창 상단의 **설정** 링크를 누릅니다.
  2. 열리는 창의 **실시간 감시** 섹션에서 **메일 안티 바이러스** 구성요소를 선택합니다.
  3. 선택한 구성요소의 **설정** 버튼을 누릅니다.
  4. 열리는 창의 **일반** 설정 탭에서 복합 파일의 감시 방식을 선택합니다.

첨부파일 필터링

이메일 첨부파일에 대한 필터 조건을 구성할 수 있습니다. 이메일을 통해 유포되는 악성 프로그램은 대부분 첨부파일로 전송되기 때문에 필터를 사용하면 컴퓨터의 보안이 강화됩니다. 특정 첨부파일 형식을 삭제하거나 이름을 바꾸면 이메일 메시지를 받을 때 자동으로 첨부파일이 열리는 것과 같은 잠재적 위험으로부터 컴퓨터를 보호할 수 있습니다.

컴퓨터가 로컬 네트워크 소프트웨어로 보호되지 않는 경우(프록시 서버 또는 방화벽 없이 직접 인터넷 접속) 첨부된 압축 파일 검사를 중지하는 않는 것이 좋습니다.

- *첨부파일 필터링 설정을 구성하려면 다음과 같이 하십시오:*

  1. 메인 프로그램 창을 열고 창 상단의 **설정** 링크를 누릅니다.
  2. 열리는 창의 **실시간 감시** 섹션에서 **메일 안티 바이러스** 구성요소를 선택합니다.
  3. 선택한 구성요소에서 **설정** 버튼을 누릅니다.
  4. 열리는 창의 첨부파일 필터 탭에서 이메일 **첨부파일의 필터링** 조건을 지정합니다. 마지막 두 가지 모드 중 하나를 선택할 경우 파일 형태 목록을 사용할 수 있고 목록에서 필요한 형식을 지정하거나 마스크를 추가하여 새로운 형식을 선택할 수 있습니다.

     새로운 형식의 마스크를 **추가**해야 할 경우 추가 링크를 누르고 열리는 **파일 이름 마스크 입력** 창에서 필요한 데이터를 입력합니다.

기본 메일 감시 설정 복원

메일 안티 바이러스를 구성할 때 항상 권장 설정을 복원할 수 있습니다. 카스퍼스키 랩에서 최적의 설정으로 권장하며 **권장 보안** 레벨로 분류됩니다.

- *기본 감시 설정을 복원하려면 다음과 같이 하십시오.*

  1. 메인 프로그램 창을 열고 창 상단의 **설정** 링크를 누릅니다.
  2. 열리는 창의 **실시간** 감시 섹션에서 **메일 안티 바이러스** 구성요소를 선택합니다.
  3. **보안 레벨** 섹션에서 선택한 구성요소에 대해 **기본값** 버튼을 누릅니다.

웹 트래픽 실시간 감시

인터넷을 사용할 때마다 컴퓨터에 저장된 정보가 위험한 프로그램에 감염될 위험이 있습니다. 이러한 프로그램은 무료 소프트웨어를 다운로드하거나 안전하지만 최근에 네트워크 공격을 받은 사이트를 이용하는 동안 컴퓨터에 침투할 수 있습니다. 또한 컴퓨터가 인터넷에 연결되어 있으므로 웹페이지를 열거나 파일을 다운로드하기 전에 네트워크 웜이 컴퓨터에 침투할 수 있습니다.

웹 안티 바이러스 구성요소는 인터넷을 사용하는 동안 보안을 제공하도록 고안되었습니다. 즉, HTTP 프로토콜을 통해 컴퓨터로 들어오는 데이터로부터 컴퓨터를 보호하고 위험한 스크립트가 컴퓨터에서 실행되지 못하도록 합니다.

웹 실시간 감시는 감시되는 포트 목록에 포함된 포트만을 통과하는 HTTP 트래픽을 감시합니다. 이메일 및 HTTP 트래픽 전송에 가장 많이 사용되는 포트 목록이 카스퍼스키 안티 바이러스 패키지에 포함되어 있습니다. 이 목록에 없는 포트를 사용하는 경우, 해당 포트를 목록에 추가하여 이러한 포트를 사용하는 트래픽을 보호해야 합니다.

비보안 영역에서 작업할 경우 인터넷에서 작업하는 동안 웹 안티 바이러스를 사용하는 것이 좋습니다. 사용 중인 컴퓨터가 HTTP 트래픽 필터 방화벽으로 보호되는 네트워크에서 실행되고 있다면 인터넷을 사용할 경우 웹 안티 바이러스가 추가 보안을 제공합니다.

보안 레벨이라는 설정 모음에 따라 트래픽 검사 방법이 결정됩니다. 웹 안티 바이러스가 보안위협을 탐지하면 지정된 처리 방법을 수행합니다.

웹 실시간 감시 레벨은 설정 그룹에 의해 결정됩니다. 설정은 다음과 같은 그룹으로 분류할 수 있습니다:

- 실시간 감시 영역 설정;
- 트래픽 실시간 감시 효율성을 확인하는 설정(휴리스틱 분석기 사용, 감시 최적화)

카스퍼스키 랩은 웹 안티 바이러스 구성요소 설정을 직접 구성하지 않을 것을 권장합니다. 대부분의 경우 다른 보안 레벨을 선택하는 것만으로 충분합니다.

- *웹 안티 바이러스 설정을 편집하려면 다음과 같이 하십시오:*

1. 메인 프로그램 창을 열고 창 상단의 **설정** 링크를 누릅니다.
2. 열리는 창의 **실시간 감시** 섹션에서 **웹 안티 바이러스** 구성요소를 선택합니다.
3. 선택한 구성요소의 **설정** 버튼을 누릅니다.
4. 구성요소 설정 중에서 필요한 사항을 변경합니다.

참조:

구성요소 연산 알고리즘 67

HTTP 트래픽 보안 레벨 변경 68

탐지된 개체에 수행할 처리 방법 변경 68

실시간 감시 영역 생성 69

검사 형태 선택 69

URL 검사 모듈 70

휴리스틱 분석기 사용 72

감시 최적화 72

기본 웹 감시 설정 복원 73

구성요소 연산 알고리즘

웹 안티 바이러스는 HTTP 를 통해 전송되는 데이터가 컴퓨터에서 위험한 스크립트를 실행하지 않도록 방지하여 컴퓨터를 보호합니다.

이 섹션에서는 구성요소 작업에 대해 자세하게 설명합니다. HTTP 트래픽은 다음 알고리즘을 통해 보호됩니다:

1. 웹 안티 바이러스가 사용자 또는 프로그램(HTTP 프로토콜을 통해)이 접근하는 각 웹 페이지/파일을 가로채서 악성 코드가 있는지 분석합니다. 악성 개체는 카스퍼스키 안티 바이러스 데이터베이스와 휴리스틱 알고리즘을 사용하여 탐지됩니다. 데이터베이스에는 현재까지 알려진 모든 악성 프로그램에 대한 설명과 이를 처리하는 방법이 포함되어 있습니다. 휴리스틱 알고리즘을 통해 데이터베이스에 아직 입력되지 않은 신종 바이러스를 탐지할 수 있습니다.

2. 분석 후에 수행할 수 있는 처리 방법은 다음과 같습니다:

   - 사용자가 접근한 웹 페이지 또는 개체에 악성 코드가 포함된 경우 접근이 차단됩니다. 그리고 요청된 개체 또는 페이지가 감염되었다는 알림이 표시됩니다.

   - 파일 또는 웹 페이지에 악성 코드가 포함되지 않은 경우 사용자에게 즉시 접근을 허락합니다.

스크립트는 다음 알고리즘에 따라 검사됩니다:

1. 웹 안티 바이러스가 웹 페이지에서 실행되는 각 스크립트를 가로채어 악성 코드가 있는지 분석합니다.

2. 스크립트에 악성 코드가 포함된 경우 웹 안티 바이러스는 이를 차단하고 사용자에게 특별한 팝업 메시지를 표시합니다.

3. 스크립트에서 악성 코드가 발견되지 않은 경우 스크립트가 실행됩니다.

스크립트 가로채기는 Microsoft Internet Explorer에서 연 웹 페이지에서만 수행됩니다.

HTTP 트래픽 보안 레벨 변경

보안 레벨은 파일 안티 바이러스 설정의 사전 설정 구성으로 정의됩니다. 카스퍼스키 랩 전문가는 세 가지 보안 레벨로 구분합니다. 사용자는 작동 조건 및 현재 상황을 토대로 레벨을 선택해야 합니다. 다음과 같은 보안 레벨 옵션 중 하나를 선택해야 합니다.

- **높음** – HTTP 를 통해 들어오는 스크립트와 개체를 가장 종합적으로 감시하는 레벨입니다. 프로그램이 프로그램 데이터베이스 전체를 사용하여 모든 개체를 완전히 검사합니다. 웹 안티 바이러스가 첨부된 압축 파일을 용량에 관계 없이 검사합니다. 검사 강도가 가장 높은 레벨에서 휴리스틱 분석기가 실행됩니다.

- **권장** – 보내고 받는 이메일을 가장 종합적으로 감시하는 레벨입니다. 웹 안티 바이러스가 첨부된 압축 파일을 용량에 관계 없이 검사합니다. 검사 강도가 가장 높은 레벨에서 휴리스틱 분석기가 실행됩니다.

- **낮음** – 가장 빠른 속도로 HTTP 트래픽과 스크립트를 검사하는 레벨입니다. 압축된 파일은 검사하지 않습니다. 검사 강도가 가장 낮은 레벨에서 휴리스틱 분석기가 실행됩니다.

세 가지 사전 설정 레벨 중 적합한 레벨이 없다면 직접 웹 안티 바이러스 설정을 구성할 수 있습니다. 결과적으로 보안 레벨 이름은 사용자지정으로 변경됩니다. 기본 구성요소 설정을 복원하려면 사전 설정된 보안 레벨 중 하나를 선택하십시오.

- *웹 트래픽의 사전 설정 보안 레벨을 변경하려면 다음과 같이 하십시오:*

1. 메인 프로그램 창을 열고 창 상단의 **설정** 링크를 누릅니다.

2. 열리는 창의 **실시간** 감시 섹션에서 **웹 안티 바이러스** 구성요소를 선택합니다.

3. 선택한 구성요소에 필요한 **보안** 레벨을 설정합니다.

탐지된 개체에 수행할 처리 방법 변경

HTTP 개체를 분석한 결과 악성 코드가 발견되면 웹 안티 바이러스 구성요소가 선택한 처리 방법에 따라 대응합니다.

웹 안티 바이러스가 항상 위험 개체의 활동을 차단하고 적용한 처리 방법을 사용자에게 알리는 팝업 메시지를 표시합니다. 위험 스크립트에 대한 처리 방법은 변경할 수 없으며 스크립트 검사 모듈 중지만 수정할 수 있습니다.

자동 모드에서 작업할 경우 위험 개체가 탐지되면 카스퍼스키 안티 바이러스는 카스퍼스키 랩의 전문가가 권장하는 처리 방법을 자동으로 적용합니다.

- *탐지된 개체에 지정된 치료 방법을 변경하려면 다음과 같이 하십시오:*

  1. 메인 프로그램 창을 열고 창 상단의 **설정** 링크를 누릅니다.
  2. 열리는 창의 **실시간** 감시 섹션에서 **웹 안티 바이러스** 구성요소를 선택합니다.
  3. 선택한 구성요소에 필요한 처리 방법을 지정합니다.

실시간 감시 영역 생성

실시간 감시 영역 생성이란 웹 안티 바이러스가 개체의 검사 형태를 선택하고 위험한 개체의 구성요소가 검사하지 않는 정보를 포함하는 신뢰하는 웹 주소 목록을 작성하는 것입니다.

따라서 절대적으로 신뢰할 수 있는 컨텐츠로 구성된 신뢰하는 웹 주소 목록을 작성할 수 있습니다. 웹 안티 바이러스는 이러한 주소의 데이터에 대해서는 위험 개체인지 여부를 분석하지 않습니다. 예를 들어, 이 옵션은 웹 안티 바이러스가 특정 파일을 다운로드하지 않는 경우에 유용할 수 있습니다.

- *신뢰하는 웹 주소 목록을 작성하려면 다음과 같이 하십시오-*

  1. 메인 프로그램 창을 열고 창 상단의 **설정** 링크를 누릅니다.
  2. 열리는 창의 실시간 **감시** 섹션에서 **웹 안티 바이러스** 구성요소를 선택합니다.
  3. 선택한 구성요소의 설정 버튼을 누릅니다.
  4. **웹 안티 바이러스** 창이 열리면 **감시 최적화** 섹션에서 신뢰하는 웹 주소의 ☑ **HTTP 트래픽은 검사 안함** 상자를 체크하고 **선택** 버튼을 누릅니다.
  5. **신뢰하는 웹 주소 목록** 창이 열리면 추가 링크를 누릅니다.
  6. **주소 마스크(URL)** 창이 열리면 신뢰하는 웹 주소(또는 신뢰하는 주소의 마스크)를 입력합니다.

검사 형태 선택

감시 영역 생성 작업에는 신뢰하는 웹 주소 목록 생성 외에 웹 안티 바이러스에서 수행하는 트래픽 검사 형태 선택도 포함됩니다. 검사 작업은 형태에 따라 스크립트 검사와 HTTP 트래픽 검사로 분류됩니다.

기본적으로 웹 안티 바이러스는 HTTP 트래픽과 스크립트를 동시에 검사합니다.

HTTP 트래픽 검사에는 바이러스 검사뿐 아니라 링크에 의심스러운 웹 주소 목록 및/또는 피싱 웹 주소 목록이 있는지 확인하기 위한 검사도 포함됩니다.

링크에 피싱 웹 주소 목록이 있는지 여부를 검사하여 일반적으로 금융 기관의 이메일 메시지를 가장하여 피싱 웹 주소로 연결되는 링크를 심어 놓는 피싱 공격을 피할 수 있습니다. 그러한 메시지 텍스트는 수신인으로 하여금 링크를 클릭하고 창이 열리면 신용 카드 번호 또는 금융 업무를 수행할 수 있는 인터넷 뱅킹 사이트의 로그인 및 암호와 같은 기밀 정보를 입력하도록 설득합니다.

피싱 사이트로 연결되는 링크는 이메일 메시지뿐 아니라 다른 방법(예: ICQ 메시지 텍스트)으로도 수신할 수 있으므로 웹 안티 바이러스 구성요소는 HTTP 트래픽 검사 수준에서 피싱 사이트에 대한 액세스 시도를 추적하여 차단합니다.

다시 말해서 링크에 의심스러운 웹 주소 목록이 있는지 검사하여 블랙 리스트에 등록된 웹사이트를 추적할 수 있습니다. 이 목록은 카스퍼스키 랩의 전문가들이 만든 것으로 프로그램 설치 패키지에 들어 있습니다.

- *웹 안티 바이러스가 스크립트를 검사할 수 있도록 하려면 다음을 수행하십시오-*

  1. 메인 프로그램 창을 열고 창 상단의 **설정** 링크를 누릅니다.
  2. 열리는 창의 **실시간** 감시 섹션에서 **웹 안티 바이러스** 구성요소를 선택합니다.
  3. 선택한 구성요소의 **설정** 버튼을 누릅니다.
  4. **웹 안티 바이러스** 창이 열리면 **고급** 설정 섹션에서 ☐ **Microsoft Internet Explorer 에서 실행되는 위험한 스크립트 차단** 상자가 선택되었는지 확인합니다. 그러면 웹 안티 바이러스가 컴퓨터에서 작업할 때 실행되는 WSH 스크립트(JavaScript, Visual Basic Script 등)뿐 아니라 Microsoft Internet Explorer 에서 처리되는 모든 스크립트를 검사합니다.

     또한 URL 검사 모듈을 사용할 수 있습니다. 이를 위해서는 ☐ **Microsoft Internet Explorer 및 Mozilla Firefox 에서 피싱 및 의심스러운 URL 여부 표시**를 체크하십시오. 그러면 웹 안티 바이러스가 브라우저(Microsoft Internet Explorer 및 Mozilla Firefox)에서 탐지된 피싱 및 의심스러운 웹 주소 URL 을 표시합니다.

- *링크에 의심스러운 웹 주소 및/또는 피싱 웹 주소가 있는지 검사하려면 다음과 같이 하십시오:*

  1. 메인 프로그램 창을 열고 창 상단의 **설정** 링크를 누릅니다.
  2. 열리는 창의 **실시간 감시** 섹션에서 **웹 안티 바이러스** 구성요소를 선택합니다.
  3. 선택한 구성요소의 **설정** 버튼을 누릅니다.
  4. **웹 안티 바이러스** 창이 열리면 **감시 방법** 섹션에서 ☐ **URL 이 의심스러운 웹 주소로 등록된 것인지 검사** 상자 및/또는 ☐ **URL 이 피싱 웹 주소로 등록된 것인지 검사** 상자가 체크되었는지 확인합니다.

카스퍼스키 URL 분석기

카스퍼스키 안티 바이러스에는 웹 안티 바이러스에서 관리하는 URL 검사 모듈이 포함되어 있습니다. 이 모듈은 웹페이지에 있는 링크가 의심스러운 웹사이트 또는 피싱 웹사이트 목록에 속해 있는지 확인합니다. 컨텐츠를 검사할

필요가 없는 신뢰하는 웹사이트 목록과 컨텐츠를 반드시 검사해야 하는 웹사이트 목록을 생성할 수 있습니다. 이 모듈은 Microsoft Internet Explorer 및 Mozilla Firefox 브라우저에 플러그인으로 포함되어 있습니다.

- *URL 검사 모듈을 작동하는 방법은 다음과 같습니다:*

  1. 메인 프로그램 창을 열고 창 상단의 **설정** 링크를 누릅니다.
  2. 열리는 창의 **실시간 감시** 섹션에서 **웹 안티 바이러스** 구성요소를 선택합니다.
  3. **보안 레벨** 섹션에서 선택한 구성요소에 대해 **설정** 버튼을 누릅니다.
  4. 열리는 웹 안티 바이러스 창의 고급 섹션에서 ☐ **Microsoft Internet Explorer 및 Mozilla Firefox 에서 피싱 및 의심스러운 URL 여부 표시** 상자를 체크합니다.

- *신뢰하는 웹사이트 목록을 생성하는 방법은 다음과 같습니다:*

  1. 메인 프로그램 창을 열고 창 상단의 **설정** 링크를 누릅니다.
  2. 열리는 창의 **실시간 감시** 섹션에서 **웹 안티 바이러스** 구성요소를 선택합니다.
  3. **보안 레벨** 섹션에서 선택한 구성요소에 대해 **설정** 버튼을 누릅니다.
  4. 열리는 **웹 안티 바이러스** 창의 **고급** 섹션에서 **설정** 버튼을 누릅니다.
  5. 열리는 카스퍼스키 툴바 창에서 ☐ 모든 웹사이트 감시 옵션을 선택하고 제외 버튼을 누릅니다.
  6. 열리는 **신뢰하는 웹사이트 목록** 창에서 **추가** 링크를 누릅니다.
  7. 열리는 **주소 마스크(URL)** 창에서 신뢰하는 웹사이트 주소 또는 마스크를 지정합니다.

- *컨텐츠를 검사해야 하는 웹사이트 목록을 생성하는 방법은 다음과 같습니다:*

  1. 메인 프로그램 창을 열고 창 상단의 **설정** 링크를 누릅니다.
  2. 열리는 창의 **실시간 감시** 섹션에서 **웹 안티 바이러스** 구성요소를 선택합니다.
  3. **보안 레벨** 섹션에서 선택한 구성요소에 대해 **설정** 버튼을 누릅니다.
  4. 열리는 **웹 안티 바이러스** 창의 **고급** 섹션에서 **설정** 버튼을 누릅니다.
  5. 열리는 카스퍼스키 툴바 창에서 ☐ **선택한 웹사이트만 감시** 옵션을 선택하고 선택 버튼을 누릅니다.
  6. 열리는 **감시할 웹사이트 목록** 창에서 **추가** 링크를 누릅니다.
  7. **열리는 주소 마스크(URL)** 창에서 웹사이트 주소 또는 마스크를 지정합니다.

휴리스틱 분석 사용

기본적으로 휴리스틱 방법은 시스템에서의 개체 활동을 분석합니다. 이러한 활동이 악성 개체에 일반적인 경우 개체는 악성 또는 감염의심으로 분류할 수 있습니다. 이 방법을 사용하면 새로운 보안위협을 바이러스 애널리스트에서 검색하기 전에 미리 탐지할 수 있습니다. 기본적으로 휴리스틱 분석기가 작동합니다.

카스퍼스키 안티 바이러스는 이메일에서 탐지된 악성 개체를 사용자에게 알립니다. 알림에 반응하여 메시지를 처리해야 합니다.

또한 검사 레벨을 기본, 자세히, 매우 자세히 등 상세하게 설정할 수 있습니다. 이렇게 하려면 슬라이더 막대를 선택한 위치로 옮겨야 합니다.

- *휴리스틱 분석기를 작동/중지하고 검사 레벨을 설정하려면 다음과 같이 하십시오:*

  1. 메인 프로그램 창을 열고 창 상단의 **설정** 링크를 누릅니다.
  2. 열리는 창의 **실시간 감시** 섹션에서 **웹 안티 바이러스** 구성요소를 선택합니다.
  3. 선택한 구성요소의 **설정** 버튼을 누릅니다.
  4. 웹 안티 바이러스 창이 열리면 감시 방법 섹션에서 ☐ 휴리스틱 분석 상자를 체크/체크해제하고 아래에서 상세 레벨을 지정합니다.

감시 최적화

악성 코드를 더 효율적으로 탐지하기 위해서 웹 안티 바이러스는 인터넷에서 다운로드되는 개체의 조각을 버퍼링합니다. 이 방법을 사용하면 웹 안티 바이러스가 다운로드가 완전히 종료된 후에만 개체를 검사하게 됩니다. 그런 다음 개체에서 바이러스를 검사하고 사용자에게 결과를 알리면 사용자가 검사 결과에 따라 허용 또는 차단 여부를 결정합니다.

그러나 개체 버퍼링를 사용하면 개체 처리 시간이 늘어나므로 프로그램이 사용자에게 개체를 반환하기까지 걸리는 시간도 늘어나게 됩니다. 따라서 대용량 개체를 복사하거나 처리할 경우 HTTP 클라이언트에 연결하는 시간이 초과될 수 있으므로 문제가 발생할 수 있습니다.

이 문제를 해결하기 위해 인터넷에서 다운로드하는 웹 개체 조각 버퍼링 시간을 제한하는 것이 좋습니다. 이 시간 제한이 만료되면 검사 없이 다운로드된 파일의 일부가 사용자에게 전송되고 개체가 완전히 복사된 후에 파일 전체가 검사됩니다. 그러므로 사용자에게 개체를 전송하는 데 필요한 시간을 줄이고 인터넷 사용을 위한 보안 레벨은 유지하면서 연결 해제 문제를 제거할 수 있습니다.

기본적으로 파일 조각 버퍼링 시간은 1 초로 제한됩니다. 이 값을 높이거나 버퍼링 시간 제한을 제거하면 바이러스 검사 효과는 높아지지만 개체에 대한 접근 속도가 다소 느려질 수 있습니다.

- *조각 버퍼링 시간 제한을 설정하거나 제거하려면 다음과 같이 하십시오:*

  1. 메인 프로그램 창을 열고 창 상단의 **설정** 링크를 누릅니다.

2. 열리는 창의 **실시간** 감시 섹션에서 **웹 안티 바이러스** 구성요소를 선택합니다.

3. 선택한 구성요소의 **설정** 버튼을 누릅니다.

4. **웹 안티 바이러스** 창이 열리면 **감시 최적화** 섹션에서 ☐ **조각 버퍼링 시간 제한** 상자를 체크/체크해제하고 오른쪽 필드에 시간 값(단위: 초)을 입력합니다.

기본 웹 감시 설정 복원

웹 안티 바이러스를 구성할 때 항상 권장 설정을 복원할 수 있습니다. 카스퍼스키 랩에서 최적의 설정으로 권장하며 **권장** 보안 레벨로 분류됩니다.

- *기본 웹 안티 바이러스 설정을 복원하려면 다음과 같이 하십시오:*

1. 메인 프로그램 창을 열고 창 상단의 **설정** 링크를 누릅니다.

2. 열리는 창의 **실시간** 감시 섹션에서 **웹 안티 바이러스** 구성요소를 선택합니다.

3. **보안 레벨** 섹션에서 선택한 구성요소에 대해 **기본값** 버튼을 누릅니다.

인스턴트 메신저 트래픽 감시

요즘 광범위하게 사용되고 있는 메신저 클라이언트(일명 IM 클라이언트)는 편리한 인터넷 서핑을 위한 추가 기능을 제공하지만 잠재적인 컴퓨터 보안 위협을 유발하기도 합니다. 의심스러운 웹사이트로 연결되거나 침입자가 피싱 공격에 사용하는 URL 이 포함된 메시지가 IM 클라이언트를 통해 전송될 수 있습니다. 악성 프로그램이 IM 클라이언트를 사용하여 스팸 메시지 및 URL 을 프로그램에 전송하여 사용자의 ID 번호와 암호를 훔칩니다.

메신저 안티 바이러스 구성요소는 IM 클라이언트가 안전한 작동할 수 있도록 보장하며 IM 프로토콜을 통해 컴퓨터로 들어오는 정보를 보호합니다.

이 제품은 ICQ, MSN, AIM, Yahoo!, Messenger, Jabber, Google Talk 등 인스턴트 메시징에 사용되는 다양한 프로그램이 안전하게 작동할 수 있도록 보장합니다.

Yahoo! Messenger와 Google Talk 프로그램은 SSL 프로토콜을 사용합니다. 메신저 안티 바이러스로 이러한 프로그램의 트래픽을 검사하려면 암호화된 연결 검사를 사용해야 합니다. 이를 위해서는 **네트워크** 섹션에서 ☐ **암호화된 연결(SSL) 검사** 상자를 체크하십시오.

조합된 설정에 따라 트래픽이 검사됩니다. 메시지에서 보안위협이 탐지될 경우 메신저 안티 바이러스가 사용자를 위해 이 메시지를 경고 메시지로 바꿉니다.

IM 트래픽 실시간 감시 레벨은 설정 그룹에 의해 결정됩니다. 설정은 다음과 같은 그룹으로 분류할 수 있습니다:

- 실시간 감시 영역 생성 설정;
- 감시 방법 결정 설정.

- *메신저 안티 바이러스 설정을 편집하려면 다음과 같이 하십시오:*

1. 메인 프로그램 창을 열고 창 상단의 **설정** 링크를 누릅니다.
2. 열리는 창의 **실시간 감시** 섹션에서 **메신저 안티 바이러스** 구성요소를 선택합니다.
3. 선택한 구성요소의 설정 중에서 필요한 사항을 변경합니다.

참조:

구성요소 연산 알고리즘 75

실시간 감시 영역 생성 75

감시 방법 선택 75

휴리스틱 분석기 사용 76

구성요소 연산 알고리즘

카스퍼스키 안티 바이러스에는 IM(인스턴트 메시징) 클라이언트를 통해 전송된 메시지에 위험 개체가 있는지 검사하는 메신저 안티 바이러스라는 구성요소가 포함되어 있습니다. 운영 체제를 시작할 때 로드되며 컴퓨터의 RAM 에서 실행되어 보내고 받는 메시지를 모두 검사합니다.

기본적으로 IM 클라이언트의 트래픽 실시간 감시는 아래에 설명된 알고리즘을 사용하여 수행됩니다:

1. 사용자가 수신하거나 전송하는 모든 메시지가 구성요소에 의해 검사됩니다.
2. 메신저 안티 바이러스는 위험 개체의 메시지 또는 의심스러운 웹 주소 및/또는 피싱 웹 주소의 데이터베이스에 등록된 URL 을 검사합니다. 보안위협이 탐지되면 메시지 텍스트가 경고 메시지로 바뀝니다.
3. 메시지에서 보안위협이 탐지되지 않으면 메시지 텍스트가 표시됩니다.

IM 클라이언트를 통해 전송된 파일을 저장하려고 시도할 경우 파일 안티 바이러스 구성요소가 파일을 검사합니다.

실시간 감시 영역 생성

실시간 감시 영역은 검사할 메시지의 형태를 의미합니다.

- ☐ **보내고 받는 모든 메시지**. 메신저 안티 바이러스는 보내고 받는 메시지를 모두 검사합니다.
- ☐ **받는 메시지**. 보내는 메시지에 위험한 개체가 포함될 가능성이 전혀 없다면 이 설정을 선택하십시오. 그러면 메신저 안티 바이러스가 받는 메시지만 검사합니다.

기본적으로 카스퍼스키 안티 바이러스는 IM 클라이언트의 보내고 받는 메시지를 모두 검사합니다.

보내는 메시지에 위험한 개체가 포함될 수 없다고 확신한다면 나가는 트래픽의 검사를 중지할 수 있습니다.

- *보내는 메시지의 검사를 중지하려면 다음과 같이 하십시오.*

1. 메인 프로그램 창을 열고 창 상단의 **설정** 링크를 누릅니다.
2. 열리는 창의 **실시간 감시** 섹션에서 **메신저 안티 바이러스** 구성요소를 선택합니다.
3. 감시 영역 섹션에서 선택한 구성요소의 ☐ **받는 메시지** 옵션을 선택합니다.

감시 방법 선택

다음과 같이 IM 클라이언트의 메시지에서 URL 을 검사하여 의심스러운 웹 주소 목록 및/또는 피싱 웹 주소 목록이 포함되어 있는지 확인하는 두 가지 감시 방법을 선택할 수 있습니다.

- ☐ **URL 이 의심스러운 웹 주소로 등록된 것인지 검사**. 메신저 안티 바이러스가 메시지 안의 링크를 검사하여 블랙 리스트 파일이 있는지 확인합니다.

- ☐ **URL 이 피싱 웹 주소로 등록된 것인지 검사**. 카스퍼스키 안티 바이러스 데이터베이스에는 현재 피싱 공격에 사용되는 것으로 알려져 있는 모든 사이트가 포함됩니다. 카스퍼스키 랩은 국제피싱대응협의체(APWG: Anti Phising Working Group)에서 확보한 주소로 이 목록을 보완합니다. 이 목록의 로컬 복사본은 카스퍼스키 안티 바이러스 데이터베이스를 업데이트할 때 함께 업데이트됩니다.

- *의심스러운 웹 주소 데이터베이스를 사용하는 메시지 안의 링크를 검사하려면 다음과 같이 하십시오.*

  1. 메인 프로그램 창을 열고 창 상단의 **설정** 링크를 누릅니다.
  2. 열리는 창의 **실시간 감시** 섹션에서 메신저 안티 바이러스 구성요소를 선택합니다.
  3. **감시 방법** 섹션에서 선택한 구성요소의 ☐ **URL 이 의심스러운 웹 주소로 등록된 것인지 검사** 상자를 체크합니다.

- *피싱 웹 주소의 데이터베이스를 사용하는 메시지 안의 링크를 검사하려면 다음과 같이 하십시오:*

  1. 메인 프로그램 창을 열고 창 상단의 **설정** 링크를 누릅니다.
  2. 열리는 창의 **실시간 감시** 섹션에서 **메신저 안티 바이러스** 구성요소를 선택합니다.
  3. 감시 방법 섹션에서 선택한 구성요소의 ☐ **URL 이 피싱 웹 주소로 등록된 것인지 검사** 상자를 체크합니다.

휴리스틱 분석기 사용

기본적으로 휴리스틱 방법은 시스템에서의 개체 활동을 분석합니다. 이를 위해 IM 클라이언트의 메시지에 포함된 스크립트가 보호된 환경에서 실행됩니다. 이러한 스크립트의 활동이 악성 개체에 일반적인 경우 개체는 악성 또는 감염의심으로 분류할 수 있습니다. 기본적으로 휴리스틱 분석기가 작동합니다.

카스퍼스키 안티 바이러스는 이메일에서 탐지된 악성 개체를 사용자에게 알립니다.

또한 검사 레벨을 **기본, 자세히, 매우 자세히** 등 상세하게 설정할 수 있습니다. 이렇게 하려면 슬라이더 막대를 선택한 위치로 옮겨야 합니다.

- *휴리스틱 분석기를 작동/중지하고 검사 레벨을 설정하려면 다음과 같이 하십시오.:*

  1. 메인 프로그램 창을 열고 창 상단의 **설정** 링크를 누릅니다.
  2. 열리는 창의 **실시간 감시** 섹션에서 **메신저 안티 바이러스** 구성요소를 선택합니다.
  3. **감시 방법** 섹션에서 ☐ **휴리스틱 분석기** 상자를 체크/체크해제하고 선택한 구성요소의 검사 레벨을 설정합니다.

사전 방역

카스퍼스키 안티 바이러스는 알려진 보안위협뿐 아니라 카스퍼스키 안티 바이러스 데이터베이스에 어떠한 정보도 없는 최신 보안위협으로부터 보호해 줍니다. 이러한 기능이 가능한 것은 사전 방역이라는 특별히 개발된 구성요소 덕분입니다.

새로운 보안위협이 컴퓨터를 손상시키기 전에 사전 방역의 사전 예방 기술이 보안위협을 처리합니다. 카스퍼스키 안티 바이러스 데이터베이스의 레코드를 기반으로 코드를 분석하는 대응 기술과는 달리 사전 예방 기술은 프로그램이 실행하는 활동의 순서를 통해 컴퓨터의 새로운 보안위협을 식별합니다. 활동 분석 결과 프로그램의 활동 순서가 의심스럽다고 판단되면 카스퍼스키 안티 바이러스가 이 프로그램의 활동을 차단합니다.

- *사전 방역 설정을 편집하려면 다음과 같이 하십시오:*

  1. 메인 프로그램 창을 열고 창 상단의 **설정** 링크를 누릅니다.
  2. 열리는 창의 **실시간 감시** 섹션에서 **사전 방역** 구성요소를 선택합니다.
  3. 선택한 구성요소 설정 중에서 필요한 사항을 변경합니다.

참조:

위험 활동 목록 사용 77

위험 활동 감시 규칙 변경 78

신뢰하는 프로그램 그룹 생성 79

시스템 계정 제어 79

위험 활동 목록 사용

Microsoft Windows XP Professional x64 Edition, Microsoft Windows Vista 또는 Microsoft Windows Vista x64 에서 카스퍼스키 안티 바이러스의 활동 제어 설정을 구성하는 방법은 다른 운영 체제를 사용할 경우와 다릅니다.

Microsoft Windows XP 에서 프로그램 활동 제어를 구성할 경우의 특성

카스퍼스키 안티 바이러스는 컴퓨터에서 실행되는 프로그램의 활동을 제어합니다. 사전 방역이 프로그램의 정의된 활동 순서에 즉각적으로 대응합니다. 예를 들어, 네트워크 리소스, 시작 폴더 또는 시스템 레지스트리에 프로그램을 복사한 다음 사본을 전송하는 등의 작업을 수행할 경우 이 프로그램이 웜이 될 가능성이 매우 높습니다. 그 밖의 위험한 작업 순서는 다음과 같습니다:

- 실행(예: 트로이 목마);

- 키보드 가로채기 시도;
- 숨겨진 드라이버 설치;
- 운영 체제 커널을 수정하려는 시도;
- 네거티브 PID 로 숨겨진 개체 및 프로세스를 생성하려는 시도;
- HOSTS 파일을 수정하려는 시도;
- 다른 프로세스를 구현하려는 시도;
- 루트킷 리디렉션 데이터 입력/출력;
- DNS 요청을 전송하려는 시도.

위험 활동 목록은 카스퍼스키 안티 바이러스가 업데이트될 때 자동으로 첨부되며 편집할 수 없습니다. 그러나 하나의 위험 활동 또는 다른 위험 활동에 대한 감시를 끌 수 있습니다.

- *하나의 위험 활동 또는 다른 위험 활동에 대한 감시를 끄려면 다음과 같이 하십시오:*

1. 메인 프로그램 창을 열고 창 상단의 **설정** 링크를 누릅니다.
2. 열리는 창의 **실시간 감시** 섹션에서 **사전 방역** 구성요소를 선택합니다.
3. 선택한 구성요소의 **설정** 버튼을 누릅니다.
4. **사전 방역** 창이 열리면 감시하지 않으려는 활동의 이름 옆에 있는 ☐ 상자를 체크해제합니다.

Microsoft Windows XP Professional x64 Edition, Microsoft Windows Vista 또는 Microsoft Windows Vista x64 에서 프로그램 활동 제어를 구성할 경우의 특성

컴퓨터가 위에 언급된 운영 체제 중 하나에서 실행되고 있을 때 각 이벤트에 제어가 적용되지 않는다면 이는 이러한 운영 체제의 특정 기능 때문입니다. 예를 들어, 다른 프로세스에 침입, 신뢰하는 프로그램을 통해 데이터 전송, 의심스러운 시스템 활동, 보호된 저장소에 접근과 같은 이벤트 형태에는 제어가 적용되지 않습니다.

위험 활동 감시 규칙 변경

위험 활동 목록은 카스퍼스키 안티 바이러스가 업데이트될 때 자동으로 첨부되며 편집할 수 없습니다. 다음과 같은 작업을 수행할 수 있습니다:

- 위험 활동 또는 기타 활동에 대한 감시 끄기;
- 사전 방역이 위험 활동을 탐지할 경우 사용하는 규칙 편집;
- 활동이 위험하지 않다고 간주하는 프로그램을 목록으로 표시하여 제외 규칙 목록 생성.

- *규칙을 변경하려면 다음과 같이 하십시오:*

  1. 메인 프로그램 창을 열고 창 상단의 **설정** 링크를 누릅니다.
  2. 열리는 창의 **실시간 감시** 섹션에서 **사전 방역** 구성요소를 선택합니다.
  3. 선택한 구성요소의 **설정** 버튼을 누릅니다.
  4. **사전 방역** 창이 열리면 **이벤트** 섹션에서 규칙을 편집할 이벤트를 선택합니다.
  5. 규칙 설명 섹션의 링크를 사용하여 선택한 이벤트의 설정을 구성합니다:
     - 사전 설정 처리 방법 링크를 누르고 **처리 방법** 선택 창이 열리면 원하는 처리 방법을 선택합니다;
     - 사전 설정 기간(활동 형태 해당 없음) 링크를 누르고 **숨겨진 프로세스 탐지** 창이 열리면 숨겨진 프로세스에 대한 검사 간격을 지정합니다;
     - 작업 실행 리포트를 생성해야 하는지 여부를 표시하려면 켜기/끄기 링크를 누릅니다.

신뢰하는 프로그램 그룹 생성

프로그램 제어 구성요소가 **신뢰하는** 그룹에 할당된 프로그램은 시스템에 보안위협을 유발하지 않습니다. 그러나 이러한 프로그램의 활동 역시 사전 방역에 의해 감시됩니다.

신뢰하는 프로그램의 범위를 지정하는 옵션을 사용해 사전 방역이 신뢰하는 프로그램의 활동을 검사하지 않도록 할 수 있습니다. 신뢰하는 프로그램에는 디지털 서명된 프로그램 또는 카스퍼스키 시큐리티 네트워크의 데이터베이스에 등록된 프로그램이 포함될 수 있습니다.

- *사전 방역이 디지털 서명된 프로그램 및/또는 카스퍼스키 시큐리티 네트워크 데이터베이스에 신뢰하는 프로그램으로 등록된 프로그램을 감시하되 해당 프로그램의 활동을 알리지 않도록 하려면 다음과 같이 하십시오:*

  1. 메인 프로그램 창을 열고 창 상단의 **설정** 링크를 누릅니다.
  2. 열리는 창의 **실시간 감시** 섹션에서 **사전 방역** 구성요소를 선택합니다.
  3. **신뢰하는 프로그램** 섹션에서 선택한 구성요소의 ☐ **디지털 서명된 프로그램 상자** 및/또는 ☐ **카스퍼스키 시큐리티 네트워크 데이터베이스**에 등록된 프로그램 상자를 체크합니다.

시스템 계정 제어

사용자 계정은 시스템에 대한 접근을 제어하고 사용자와 해당 작업 환경을 확인하여 다른 사용자가 운영 체제 또는 데이터를 손상시키지 못하도록 합니다. 시스템 프로세스는 시스템 사용자 계정에 의해 실행되는 프로세스입니다.

- *카스퍼스키 안티 바이러스를 통해 사용자 프로세스 외에 시스템 프로세스의 활동을 감시하려면 다음과 같이 하십시오:*

  1. 메인 프로그램 창을 열고 창 상단의 **설정** 링크를 누릅니다.
  2. 열리는 창의 **실시간 감시** 섹션에서 **사전 방역** 구성요소를 선택합니다.
  3. **고급 설정** 섹션에서 선택한 구성요소의 ☐ **시스템 사용자 계정 감시** 상자를 체크합니다.

컴퓨터 검사

컴퓨터의 바이러스 및 취약점 검사는 컴퓨터의 보안을 보장하는 가장 중요한 작업 중 하나입니다. 바이러스 검사는 몇 가지 이유로 악성 프로그램 실시간 감시에 의해 탐지되지 않는 악성 코드의 확산을 탐지합니다. 취약점 검사는 침입자가 악성 개체를 퍼뜨리고 개인 정보에 대한 접근 권한을 얻는 데 사용할 수 있는 소프트웨어 취약점을 탐지합니다.

카스퍼스키 랩의 전문가들은 이동식 드라이브 검사를 포함한 바이러스 검사 작업과 시스템 및 프로그램의 취약점 검사를 구분합니다.

- *검사 작업의 설정을 변경하려면 다음과 같이 하십시오.:*

  1. 메인 프로그램 창을 열고 창 상단의 설정 링크를 누릅니다.
  2. 창 왼쪽의 수동 검사(**컴퓨터 전체 검사, 빠른 검사, 개체 검사, 취약점 검사**) 섹션에서 필요한 작업을 선택합니다.
  3. 선택한 작업의 설정 중에서 필요한 사항을 변경합니다.

참조:

바이러스 검사 81
취약점 검사 92

바이러스 검사

카스퍼스키 랩 전문가는 바이러스 검사 작업을 다음 몇 가지로 구분합니다.

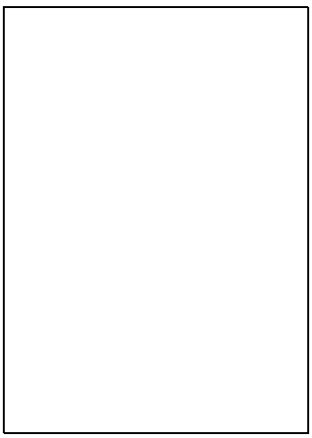
- **개체 검사.** 사용자가 선택한 개체가 검사됩니다. 컴퓨터 파일 시스템에 있는 아무 개체나 검사 가능합니다. 이 작업에서는 이동식 드라이브에 대한 검사 설정도 구성할 수 있습니다.
- **컴퓨터 전체 검사.** 전체 컴퓨터를 완전히 검사합니다. 기본적으로 시스템 메모리, 시작 시 로딩된 프로그램, 시스템 백업, 이메일 데이터베이스, 하드 드라이브, 이동식 저장 장치, 네트워크 드라이브 등은 검사 대상입니다.
- **빠른 검사.** 운영 체제 시작 개체가 검사됩니다.

전체 검사 및 빠른 검사 작업은 정해진 작업입니다. 이 작업에서 검사되는 개체 목록을 변경하지 않는 것이 좋습니다.

각 검사 작업은 지정한 영역에서 수행하며 생성된 스케줄에 따라 실행할 수 있습니다. 바이러스 검사 작업 파라미터 집합을 통해 보안 레벨을 정의할 수 있습니다. 기본적으로 세 가지 레벨이 제공됩니다.

바이러스 검사 작업 시작 후에는 메인 프로그램 창 **수동 검사** 섹션의 시작된 작업 이름 아래 **마지막 시작 시간** 칸에 진행률이 표시됩니다. 보안위협이 탐지되는 경우 지정된 처리 방법이 수행됩니다.
보안위협을 검색하는 동안 결과 정보는 카스퍼스키 안티 바이러스 리포트에 기록됩니다.

또한 Microsoft Windows 운영 체제의 표준 도구(예: **탐색기** 프로그램 창 또는 **바탕 화면** 등)를 사용하여 바이러스를 검사할 개체를 선택할 수도 있습니다. 검사할 개체 이름에 커서를 가져가서 마우스 오른쪽 버튼을 눌러 Microsoft Windows 마우스 오른쪽 메뉴를 연 다음 **바이러스 검사 옵션**을 선택합니다.



Microsoft Windows 마우스 오른쪽 메뉴

또한 작업 실행 중에 발생한 이벤트에 대한 전체 정보가 포함된 검사 리포트를 볼 수도 있습니다.

참조:

바이러스 검사 시작 83
작업 실행 바로가기 생성 84
검사할 개체 목록 생성 84
보안 레벨 변경 85
탐지된 개체에 수행할 처리 방법 변경 86
검사할 개체 형태 변경 86
감시 최적화 87
이동식 디스크 드라이브 검사 88
복합 파일 검사 88
고급 감시 기술 89
감시 방법 변경 90
스케줄: 스케줄 생성 90
스케줄: 계정 지정 91
스케줄된 작업 실행 기능 91
기본 검사 설정 복원 92

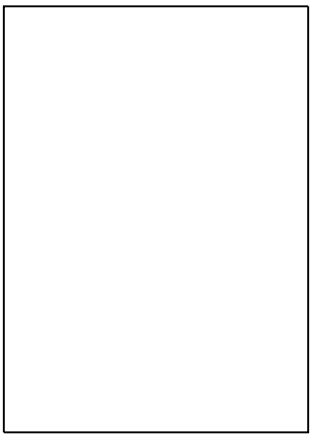
바이러스 검사 작업 시작

다음 중 한 가지 방법을 사용하여 바이러스 검사 작업을 시작할 수 있습니다.:

- 카스퍼스키 안티 바이러스 마우스 오른쪽 메뉴 사용
- 카스퍼스키 안티 바이러스 메인 창 사용
- 이전에 생성한 바로가기 사용

작업 정보가 카스퍼스키 안티 바이러스의 메인 창에 표시됩니다.

또한 Microsoft Windows 운영 체제의 표준 도구를 사용하여 검사할 개체를 선택할 수 있습니다(예: **Explorer** 프로그램 창 또는 **바탕화면** 등).



Microsoft Windows 마우스 오른쪽 메뉴

- *바로가기를 사용하여 작업을 시작하려면:*

  1. 바로가기가 만들어진 폴더를 엽니다.
  2. 바로가기를 더블클릭하여 작업을 시작합니다. 작업 실행 진행 상황이 **수동 검사** 섹션의 카스퍼스키 안티 바이러스 메인 창에 표시됩니다.

- *프로그램의 마우스 오른쪽 메뉴에서 바이러스 검사 작업을 시작하려면:*

  1. 작업 표시줄 알림 영역에서 프로그램 아이콘을 마우스 오른쪽 버튼으로 누릅니다.
  2. 열리는 마우스 오른쪽 메뉴에서 **바이러스 검사** 항목을 선택합니다.
  3. **수동 검사** 섹션에 카스퍼스키 안티 바이러스 메인 창이 열리면 원하는 작업의 이름이 표시된 버튼을 누릅니다.

컴퓨터 전체 검사를 시작하려면 마우스 오른쪽 메뉴에서 **컴퓨터 전체 검사** 항목을 선택합니다. 그러면 컴퓨터 전체 검사가 시작됩니다. 작업 실행 진행 상황이 **수동 검사** 섹션의 카스퍼스키 안티 바이러스 메인 창에 표시됩니다.

- *메인 프로그램 창에서 바이러스 검사 작업을 시작하려면:*

  1. 메인 프로그램 창을 엽니다.
  2. 창 왼쪽에서 수동 검사 섹션을 선택합니다.
  3. 원하는 작업의 이름이 표시된 버튼을 누릅니다.

- *Microsoft Windows 의 마우스 오른쪽 메뉴에서 선택한 개체의 바이러스 검사 작업을 시작하려면:*

  1. 선택한 개체의 이름을 마우스 오른쪽 버튼으로 누릅니다.
  2. 열리는 마우스 오른쪽 메뉴에서 **바이러스 검사** 항목을 선택합니다. 작업 실행 진행 상황 및 결과가 열리는 창에 표시됩니다.

작업 실행 바로가기 생성

프로그램이 컴퓨터 전체 검사 작업과 빠른 검사 작업을 빠르게 시작할 수 있는 바로가기 생성 옵션을 제공합니다. 이 옵션을 사용하여 메인 프로그램 창이나 마우스 오른쪽 메뉴를 열지 않고도 원하는 검사 작업을 시작할 수 있습니다.

- *검사 작업 시작을 위한 바로가기를 생성하려면 다음과 같이 하십시오.*

  1. 메인 프로그램 창을 열고 창 상단의 **설정** 링크를 누릅니다.
  2. 창 왼쪽에서 **수동 검사** 섹션을 선택합니다.
  3. 창 오른쪽의 **수동 검사 작업 바로가기** 블록에서 원하는 작업의 이름(**빠른 검사** 또는 **컴퓨터 전체 검사**) 옆에 있는 **바로가기 만들기** 버튼을 누릅니다.
  4. 열리는 창에서 바로가기를 저장할 경로와 이름을 지정합니다. 기본적으로 바로가기는 선택한 작업의 이름으로 현재 컴퓨터 사용자의 *내 컴퓨터* 폴더에 생성됩니다.

검사할 개체 목록 생성

바이러스 검사 작업마다 기본 개체 목록이 있습니다. 이러한 개체에는 논리 드라이브, **이메일 데이터베이스**와 같은 컴퓨터 파일 시스템의 항목 또는 네트워크 드라이브와 같은 다른 형태의 개체가 포함될 수 있습니다. 이 목록은 편집할 수 있습니다.

개체를 추가하면 즉시 목록에 나타납니다. 개체를 추가할 때 ☑ **하위폴더 포함** 상자가 선택된 경우 반복해서 검사를 실행합니다.

목록에서 개체를 삭제하려면 개체를 선택하고 **삭제** 링크를 누릅니다.

기본적으로 목록에 표시되는 개체는 편집 또는 삭제할 수 없습니다.

목록에서 개체를 삭제할 뿐 아니라 검사를 실행할 때 일시적으로 개체를 건너뛸 수 있습니다. 이렇게 하려면 목록에서 개체를 선택하고 개체의 이름 옆에 있는 상자를 체크해제하십시오.

검사 영역이 비었거나 선택한 개체가 없을 경우 검사 작업을 시작할 수 없습니다!!

- *개체 검사 작업에 사용할 개체의 목록을 생성하려면 다음과 같이 하십시오.:*

  1. 메인 프로그램 창을 엽니다.
  2. 창 왼쪽에서 **수동 검사** 섹션을 선택합니다.
  3. 추가 **링크**를 누릅니다.
  4. **검사할 개체 선택** 창이 열리면 개체를 선택하고 **추가** 버튼을 누릅니다. 필요한 개체를 모두 추가한 후 **확인** 버튼을 누릅니다. 검사 대상 개체 목록에서 개체를 제외시키려면 해당 개체 옆에 있는 상자를 체크해제합니다.

- *빠른 검사 또는 컴퓨터 전체 검사 작업에 사용할 개체의 목록을 생성하려면 다음과 같이 하십시오:*

  1. 메인 프로그램 창을 열고 창 상단의 **설정** 링크를 누릅니다.
  2. 창 왼쪽에서 컴퓨터 **전체 검사**(**빠른 검사**) 작업을 선택합니다.
  3. **검사 영역** 블록에서 선택한 작업의 **설정** 버튼을 누릅니다.
  4. **<검사 작업 이름>: 개체 목록** 창이 열리면 **추가, 편집, 삭제** 링크를 사용하여 목록을 생성합니다. 검사 대상 개체 목록에서 개체를 제외시키려면 해당 개체 옆에 있는 상자를 체크해제합니다.

보안 레벨 변경

보안 레벨은 사전에 설정된 검사 설정 모음입니다. 카스퍼스키 랩 전문가는 보안 레벨을 세 가지로 구분합니다. 사용자는 환경 설정에 따라 어떤 레벨을 선택할지 결정해야 합니다. 다음 보안 레벨 중 하나를 선택할 수 있습니다:

- **높음.** 컴퓨터의 감염 위험이 높다고 판단될 경우 이 레벨을 사용하십시오.
- **권장.** 이 레벨은 대부분의 경우에 적합하며 카스퍼스키 랩 전문가들이 권장하는 레벨입니다.
- **낮음.** 이 모드에서는 프로그램이 시스템 리소스 사용이 최소화되므로 RAM 리소스가 많이 필요한 프로그램을 사용할 경우 낮은 보안 레벨을 선택하십시오.

세 가지 사전 설정 레벨 중 적합한 레벨이 없을 경우 검사 설정을 직접 구성할 수 있습니다. 결과적으로 보안 레벨 이름은 **사용자 지정**으로 변경됩니다. 기본 검사 설정을 복원하려면 사전 설정된 보안 레벨 중 하나를 선택하십시오

- *정의된 보안 레벨을 변경하려면 다음과 같이 하십시오:*

  1. 메인 프로그램 창을 열고 창 상단의 **설정** 링크를 누릅니다.
  2. 창 왼쪽의 **수동 검사(컴퓨터 전체 검사**, **빠른 검사**, **수동 검사**) 섹션에서 필요한 작업을 선택합니다.

3. **보안 레벨** 섹션에서 선택한 작업에 필요한 보안 레벨을 설정합니다.

탐지된 개체에 수행할 처리 방법 변경

보안위협이 탐지되면 카스퍼스키 안티 바이러스가 이를 다음 상태 중 하나로 지정합니다:

- 악성 프로그램(*바이러스* 또는 *트로이 목마* 등)
- *감염 위험 상태(검사 결과 개체가 감염되었는지 여부를 결정할 수 없는 경우). 이 작업은 프로그램이 파일에서 알려지지 않은 바이러스의 코드 또는 알려진 바이러스의 변형된 코드를 탐지한 경우에 수행됩니다.*

카스퍼스키 안티 바이러스는 바이러스 검사 도중 감염 개체 또는 감염 위험 개체를 탐지한 경우 이를 사용자에게 알립니다. 개체에 수행할 처리 방법을 선택하여 신종 보안위협에 대응해야 합니다. 카스퍼스키 안티 바이러스는 탐지된 개체에 대한 처리 방법으로 기본 설정인 **사용자 확인 후 처리 옵션**을 선택합니다. 처리 방법은 변경할 수 있습니다. 예를 들어, 탐지된 각 개체를 치료해야 하고 감염된 개체나 의심스러운 개체가 탐지되었다는 알림을 수신할 때마다 **치료** 처리 방법을 선택하지 않으려면 **사용자 확인 없이 치료**를 선택하십시오.

탐지된 개체를 치료하거나 삭제하기 전에 카스퍼스키 안티 바이러스는 이후 초기화 또는 치료를 허락하기 위해 개체의 백업 복사본을 생성합니다.

자동 모드에서 작업할 경우 위험 개체가 탐지되면 카스퍼스키 안티 바이러스가 카스퍼스키 랩의 전문가가 권장하는 처리 방법을 자동으로 적용합니다. 악성 개체의 경우 치료 방법은 **치료**이고, **삭제해야 치료되는 것은 삭제**이며, 감염의심 개체의 경우 **건너뛰기**입니다.

- *탐지된 개체에 지정된 치료 방법을 변경하려면 다음과 같이 하십시오:*

1. 메인 프로그램 창을 열고 창 상단의 설정 **링크**를 누릅니다.
2. 창 왼쪽의 **수동 검사**(**컴퓨터 전체 검사**, **빠른 검사**, **개체 검사**) 섹션에서 필요한 작업을 선택합니다.
3. **처리 방법** 블록에서 선택한 작업에 필요한 처리 방법을 지정합니다.

검사할 개체 형태 변경

검사할 개체 형태를 지정할 경우 선택한 검사 작업을 실행할 때 바이러스를 검사할 파일 형식과 크기를 결정해야 합니다.

파일 형태를 선택할 때 다음 사항을 기억해야 합니다:

- 악성 코드가 여러 파일 형식(예: .txt)으로 침투하지만 그 이상 활성화될 가능성이 매우 낮은 경우가 있습니다. 이와 동시에 실행 코드(예: .exe, .dll, .doc)를 포함하거나 포함할 수 있는 형식이 있습니다. 그러한 파일은 악성 코드가 침투하여 활성화될 위험이 매우 높습니다.a

- 침입자가 확장자가 *.txt* 인 파일(실제로는 *.txt* 파일로 이름을 변경한 실행 파일)에 바이러스를 심어 컴퓨터로 전송할 수 있다는 점을 기억하십시오. **감염 가능성이 높은 파일 - 알려진 확장자** 옵션을 선택한 경우 이러한 파일은 검사에서 생략됩니다 **감염 가능성이 높은 파일 - 확장자 분석** 옵션을 선택한 경우 파일 실시간 감시가 파일 헤더를 분석하여 .exe 파일인지 확인할 수 있습니다. 그러한 파일은 바이러스가 있는지 철저하게 검사됩니다.

- *검사되는 개체의 형태를 변경하려면 다음과 같이 하십시오:*

  1. 메인 프로그램 창을 열고 창 상단의 **설정** 링크를 누릅니다.
  2. 창 왼쪽의 **수동 검사**(**컴퓨터 전체 검사**, **빠른 검사**, **개체 검사**) 섹션에서 필요한 작업을 선택합니다.
  3. **보안 레벨** 섹션에서 선택한 작업의 **설정** 버튼을 누릅니다.
  4. 열리는 창의 **영역** 탭 아래 있는 **감시 파일 형태** 섹션에서 필요한 설정을 선택합니다.

검사 최적화

검사 시간을 단축하고 카스퍼스키 안티 바이러스의 속도를 높일 수 있습니다. 새 파일과 마지막 검사 후 변경된 파일만 검사하여 검사 시간을 단축할 수 있습니다. 이 모드는 단순 파일과 복합 파일 모두에 적용됩니다.

이 외에도 검사 지속 시간에 제한을 설정할 수 있습니다. 지정된 시간이 경과하면 파일 검사가 중지됩니다.

- *새로운 것이나 변경된 파일만 검사하려면 다음과 같이 하십시오:*

  1. 메인 프로그램 창을 열고 창 상단의 **설정** 링크를 누릅니다.
  2. 창 왼쪽의 **수동 검사**(**컴퓨터 전체 검사**, **빠른 검사**, **개체 검사**) 섹션에서 필요한 작업을 선택합니다.
  3. **보안 레벨** 섹션에서 선택한 작업의 **설정** 버튼을 누릅니다.
  4. 열리는 창의 **영역** 탭 아래 있는 **검사 최적화** 섹션에서 **새로운 것이나 변경된 파일만 감시** 상자를 체크합니다.

- *검사 지속 시간에 시간 제한을 적용하려면 다음과 같이 하십시오.*

  1. 메인 프로그램 창을 열고 창 상단의 **설정** 링크를 누릅니다.
  2. 창 왼쪽의 **수동 검사**(**컴퓨터 전체 검사**, **빠른 검사**, **개체 검사**) 섹션에서 필요한 작업을 선택합니다.
  3. **보안 레벨** 섹션에서 선택한 작업의 **설정** 버튼을 누릅니다.
  4. 열리는 창의 영역 탭 아래 있는 **검사 최적화** 섹션에서 **다음보다 오래 걸리는 것은 검사 중지** 상자를 체크하고 옆에 있는 필드에서 검사 지속 시간을 지정합니다.

이동식 디스크 드라이브 검사

요즘은 운영 체제의 취약점을 이용해 네트워크 및 이동식 장치를 통해 복사하는 악성 개체가 점점 더 확산되고 있습니다.

이동식 드라이브가 컴퓨터에 연결되어 있을 경우 이동식 드라이브 검사 옵션을 사용할 수 있습니다. 이렇게 하려면 카스퍼스키 안티 바이러스에 의해 수행되는 처리 방법 중 하나를 선택해야 합니다:

- **검사 안함.** 이동식 드라이브가 컴퓨터에 연결되어 있는 경우에도 이동식 드라이브를 자동으로 검사하지 않습니다.
- **사용자에게 확인.** 기본적으로 카스퍼스키 안티 바이러스는 이동식 장치를 연결할 때 사용자에게 추가 단계를 수행할지 물어봅니다.
- **컴퓨터 전체 검사.** 이동식 드라이브를 연결할 때 프로그램이 컴퓨터 전체 검사의 설정에 따라 이동식 장치에 저장된 모든 파일을 검사할지 물어봅니다.
- **빠른 검사**. 이동식 장치를 연결할 때 빠른 검사의 설정에 따라 자동 시작 개체만 검사됩니다.

- *이동식 장치를 연결할 때 이동식 장치 검사 기능을 사용하려면 다음과 같이 하십시오.*

  1. 메인 프로그램 창을 열고 창 상단의 **설정** 링크를 누릅니다.
  2. 창 왼쪽에서 **수동 검사** 섹션을 선택합니다.
  3. **이동식 장치가 연결될 때 검사** 블록에서 처리 방법을 선택하고 필요한 경우 아래 필드에서 검사하는 드라이브의 최대 크기를 정의합니다.

복합 파일 검사

바이러스를 숨기는 일반적인 방법은 바이러스를 압축 파일, 데이터베이스 등의 복합 파일에 끼워 넣는 것입니다. 이러한 방법으로 숨겨진 바이러스를 탐지하려면 검사 속도를 크게 저하시킬 수 있는 복합 파일을 압축해제해야 합니다.

각 복합 파일 형태에 대해 모든 파일을 검사할지 또는 새 파일만 검사할지 선택할 수 있습니다. 이렇게 하려면 개체 이름 옆에 있는 링크를 사용하십시오. 이 링크를 마우스 왼쪽 버튼으로 눌러 값을 변경할 수 있습니다. 새로운 것이나 변경된 파일만 검사 감시 방식을 선택하면 검사되는 복합 파일의 형태를 선택할 수 없게 됩니다.

검사되는 복합 파일의 최대 크기를 제한할 수 있습니다. 지정된 값보다 큰 복합 파일은 검사되지 않습니다.

압축해제한 대용량 파일은 ☑ **다음보다 큰 복합 파일은 압축해제 안함** 상자가 체크된 경우에도 검사됩니다.

- *검사되는 복합 파일의 목록을 수정하려면 다음과 같이 하십시오.*

  1. 메인 프로그램 창을 열고 창 상단의 **설정** 링크를 누릅니다.
  2. 창 왼쪽의 **수동 검사**(**컴퓨터 전체 검사, 빠른 검사, 개체 검사**) 섹션에서 필요한 작업을 선택합니다.
  3. **보안 레벨** 섹션에서 선택한 작업의 **설정** 버튼을 누릅니다.
  4. 열리는 창의 **영역** 탭 아래 있는 **복합 파일 검사** 섹션에서 검사할 복합 파일의 형태를 선택합니다.

- *검사되는 복합 파일의 최대 크기를 설정하려면 다음과 같이 하십시오.*

  1. 메인 프로그램 창을 열고 창 상단의 **설정** 링크를 누릅니다.
  2. 창 왼쪽의 **수동 검사**(**컴퓨터 전체 검사, 빠른 검사, 개체 검사**) 섹션에서 필요한 작업을 선택합니다.
  3. **보안 레벨** 섹션에서 선택한 작업의 **설정** 버튼을 누릅니다.
  4. 열리는 창의 **영역** 탭 아래 있는 **복한 파일 검사** 섹션에서 **고급 설정** 버튼을 누릅니다.
  5. **복합 파일** 창이 열리면 ☑ **다음보다 큰 복합 파일은 압축해제 안함** 상자를 체크하고 아래 필드에서 파일 크기를 지정합니다.

고급 감시 기술

또한 검사 중에 사용되는 기술을 지정할 수 있습니다. 다음 기술 중 하나를 선택할 수 있습니다.

- **iChecker**. 이 기술은 특정 개체를 검사에서 제외하여 검사 속도를 높일 수 있습니다. 개체는 프로그램 데이터베이스 배포 날짜, 마지막 개체 검사 날짜, 스캔 설정 변경 사항 등을 고려하는 특별 알고리즘을 사용하여 검사에서 제외됩니다.

  예를 들어, 검사 후 카스퍼스키 안티 바이러스가 *감염되지 않음* 상태를 할당한 압축 파일이 있다고 가정해 보겠습니다. 이 압축 파일이 바뀌거나 검사 설정이 변경되지 않은 경우 프로그램은 다음 번에 이 압축 파일을 건너뜁니다. 그러나 새 개체가 압축 파일에 추가되어 압축 파일의 구조가 변경되거나 검사 설정이 변경되거나 프로그램 데이터베이스가 업데이트된 경우 프로그램이 압축 파일을 다시 검사합니다.

  iChecker 에는 몇 가지 제한이 있습니다. 예를 들어, 대용량 파일에서는 사용할 수 없으며 프로그램에서 인지하는 구조로 된 개체(예: exe, .dll, .lnk, .ttf, .inf, .sys, .com, .chm, .zip, .rar)에만 적용됩니다.

- **iSwift**. 이 기술은 NTFS 파일 시스템을 사용하는 컴퓨터를 위해 iChecker 기술을 발전시킨 것입니다. iSwift 에는 몇 가지 제한이 있습니다. 파일 시스템의 특정 파일 위치에만 해당되므로 NTFS 에 있는 개체에만 적용할 수 있습니다.

- *고급 개체 감시 기술을 변경하려면 다음과 같이 하십시오.*

  1. 메인 프로그램 창을 열고 창 상단의 **설정** 링크를 누릅니다.
  2. 창 왼쪽의 **수동 검사**(**컴퓨터 전체 검사, 빠른 검사, 개체 검사**) 섹션에서 필요한 작업을 선택합니다.

3. **보안 레벨** 섹션에서 선택한 작업의 **설정** 버튼을 누릅니다.

4. 열리는 창의 **고급 설정** 탭 아래 있는 **고급 감시 기술** 섹션에서 원하는 설정 값을 선택합니다.

검사 방법 변경

검사 설정을 편집하여 철저하게 검사할 수 있습니다. 기본적으로 프로그램 데이터베이스 레코드를 사용하여 보안위협을 검사하는 모드가 항상 활성화되어 있습니다. 또한 다양한 감시 방법과 고급 감시 기술을 적용할 수 있습니다.

카스퍼스키 안티 바이러스가 탐지된 개체와 데이터베이스 레코드를 비교하는 검사 방식을 *시그니처 분석*이라고 하며 이 모드는 항상 사용됩니다. 또한 항상 *휴리스틱 분석기*를 사용할 수 있습니다. 이 방법은 개체가 시스템 내에서 수행하는 활동의 분석 결과를 추론합니다. 이러한 활동이 악성 개체에 일반적인 경우 개체는 악성 또는 감염의심으로 분류할 수 있습니다.

또한 휴리스틱 분석 레벨을 기본, 자세히, 매우 자세히 등 상세하게 설정할 수 있습니다. 이렇게 하려면 슬라이더 막대를 선택한 위치로 옮겨야 합니다.

이러한 검사 방법 외에 루트킷 검사도 사용할 수 있습니다. 루트킷은 운영 체제에 악성 프로그램을 숨길 수 있는 도구 세트입니다. 이러한 유틸리티는 시스템에 삽입되어 숨겨진 상태로 루트킷이 설치된 다른 악성 프로그램의 프로세스, 폴더, 레지스트리 키를 숨깁니다. 검사가 작동 중인 경우 여러 다양한 개체를 분석하여 이러한 프로그램을 세밀하게 검사하는 상세 레벨(고급 분석)을 지정하여 루트킷을 탐지할 수 있습니다.

- *사용할 검사 방법 을 지정하려면 다음과 같이 하십시오.*

  1. 메인 프로그램 창을 열고 창 상단의 **설정** 링크를 누릅니다.

  2. 창 왼쪽의 **수동 검사**(**컴퓨터 전체 검사, 빠른 검사, 개체 검사**) 섹션에서 필요한 작업을 선택합니다.

  3. **스케줄** 섹션에서 선택한 작업의 **설정** 버튼을 누릅니다.

  4. 열리는 창의 **고급 설정** 탭 아래 있는 **검사 방법** 섹션에서 원하는 설정 값을 선택합니다.

스케줄: 스케줄 생성

바이러스 검사 작업을 자동으로 시작할 스케줄을 생성할 수 있습니다.

선택할 주요 항목은 작업 자동 시작 사이의 시간 간격입니다. 빈도를 변경하려면 선택한 옵션의 스케줄 설정을 지정하십시오.

컴퓨터의 전원이 켜져 있지 않는 등 다양한 이유로 작업을 시작할 수 없는 경우 컴퓨터의 전원이 켜지면 자동으로 시작하도록 작업을 구성할 수 있습니다.

- *검사 작업의 스케줄을 편집하려면 다음과 같이 하십시오.*

  1. 메인 프로그램 창을 열고 창 상단의 **설정** 링크를 누릅니다.

  2. 창 왼쪽의 **수동 검사**(**컴퓨터 전체 검사, 빠른 검사, 개체 검사**) 섹션에서 필요한 작업을 선택합니다.

3. **스케줄** 섹션에서 선택한 작업의 **설정** 버튼을 누릅니다.
4. 가장 적합한 시간에 검사 작업을 시작하려면 열리는 창의 **스케줄** 탭 아래 있는 **스케줄** 섹션에서 **수동 시작** 옵션을 선택합니다. 주기적으로 작업을 실행하려면 **스케줄 시작**을 선택하고 작업 실행 스케줄을 생성합니다.

- *건너뛴 작업을 자동으로 실행하도록 구성하려면 다음과 같이 하십시오.*

1. 메인 프로그램 창을 열고 창 상단의 **설정** 링크를 누릅니다.
2. 창 왼쪽의 **수동 검사**(**컴퓨터 전체 검사, 빠른 검사, 개체 검사**) 섹션에서 필요한 작업을 선택합니다.
3. **스케줄** 섹션에서 선택한 작업의 **설정** 버튼을 누릅니다.
4. 열리는 창의 **스케줄** 탭 아래 있는 **스케줄** 섹션에서 ☑ **건너뛴 작업 실행** 상자를 체크합니다.

스케줄: 계정 지정

바이러스 검사를 수행할 때 프로그램이 사용할 계정을 지정할 수 있습니다.

- *계정을 지정하려면:*

1. 메인 프로그램 창을 열고 창 상단의 **설정** 링크를 누릅니다.
2. 창 왼쪽의 **수동 검사**(**컴퓨터 전체 검사, 빠른 검사, 개체 검사**) 섹션에서 필요한 작업을 선택합니다.
3. **스케줄** 섹션에서 선택한 작업의 **설정** 버튼을 누릅니다.
4. 열리는 창의 **스케줄** 탭 아래 있는 **사용자 계정** 섹션에서 ☑ **다음 계정으로 작업 실행** 상자를 체크하고 사용자 이름 및 암호를 지정합니다.

스케줄된 작업 실행 기능

모든 검사 작업을 수동으로 또는 스케줄에 따라 시작할 수 있습니다.

예를 들어, 스케줄된 작업에 대해 *스크린세이버 기능이 중지되어 있거나 컴퓨터가 잠금 해제되어 있다면 스케줄된 검사 일시 중지* 등의 추가 기능을 사용할 수 있습니다. 이 기능은 사용자가 컴퓨터에서 작업을 완료할 때까지 작업 실행을 연기합니다. 따라서 작업 중에는 검사 작업이 시스템 리소스를 점유하지 않습니다.

- *컴퓨터를 더 이상 사용하지 않을 경우에만 검사 작업을 실행하려면 다음과 같이 하십시오:*

1. 메인 프로그램 창을 열고 창 상단의 **설정** 링크를 누릅니다.
2. 창 왼쪽의 **수동 검사**(**컴퓨터 전체 검사, 빠른 검사, 개체 검사**) 섹션에서 필요한 작업을 선택합니다.
3. **스케줄** 섹션에서 선택한 작업의 **설정** 버튼을 누릅니다.

4. 열리는 창의 **스케줄** 탭 아래 있는 **스케줄** 섹션에서 **스크린세이버 기능이 중지되어 있거나 컴퓨터가 잠금 해제되어 있다면 스케줄된 검사 일시 중지** 상자를 체크합니다.

기본 검사 설정 복원

작업 설정을 구성할 경우 언제든지 권장 설정을 복원할 수 있습니다. 카스퍼스키 랩에서 최적의 설정으로 권장하며 **권장** 보안 레벨로 분류됩니다.

- *기본 파일 검사 설정을 복원하려면:*

1. 메인 프로그램 창을 열고 창 상단의 **설정** 링크를 누릅니다.
2. 창 왼쪽의 **수동 검사**(**컴퓨터 전체 검사, 빠른 검사, 개체 검사**) 섹션에서 필요한 작업을 선택합니다.
3. **보안 레벨** 섹션에서 선택한 작업의 **기본 값** 버튼을 누릅니다.

취약점 검사

취약점 검사 작업은 시스템 보안 진단과 침입자가 컴퓨터를 손상시키기 위해 일반적으로 사용하는 잠재적인 취약점 검색으로 구성됩니다.

취약점을 검사할 때 프로그램이 시스템을 분석하고 운영 체제 및 브라우저 설정에서 예외나 손상을 검색합니다. 보안 진단은 루트킷 설치(예: 해킹되는 시스템을 비밀리에 감시하는 프로그램) 검색, 취약한 서비스 및 설정 검색, 프로세스 및 드라이버에 대한 정보 수집 등의 여러 가지 측면으로 구성됩니다.

시스템 취약점 진단은 다소 시간이 걸릴 수 있습니다. 진단이 완료되면 수집된 정보를 분석하여 시스템에서 발생할 수 있는 보안위협의 관점에서 보안 문제를 평가합니다.

시스템 분석 단계에서 탐지된 모든 문제는 위험도별로 그룹화됩니다. 카스퍼스키 랩이 시스템 설정에서 취약점을 제거할 수 있도록 각 문제 그룹에 적합한 처리 방법을 제공합니다. 문제는 세 가지 그룹으로 분류할 수 있으며 각각의 문제에 맞게 치료 방법도 세 가지 그룹이 있습니다:

- *강력히 권장하는 처리 대상*은 심각한 보안위협으로 게시되는 문제를 제거하는 데 도움이 됩니다. 사용자는 이 그룹에 속한 모든 처리 방법을 수행하는 것이 좋습니다.
- *권장 처리 대상*은 잠재적 보안위협으로 게시되는 문제를 제거하는 데 도움이 됩니다. 사용자는 이 그룹에 속한 처리 방법도 모두 수행하는 것이 좋습니다.
- *추가 처리 대상*은 현재는 위협이 되지 않지만 이후에 컴퓨터의 보안을 위협할 수 있는 시스템 손상을 복구하는 데 도움이 됩니다.

운영 체제와 설치된 사용자 프로그램에서 잠재적인 취약점을 검색한 결과가 중요 수정 프로그램(프로그램 업데이트)으로 연결되는 직접 링크로 표시됩니다.

취약점 검사 작업이 시작되면 실행 프로세스가 메인 프로그램 창과 **완료 예상 시간** 필드의 **취약점 검사** 창에 표시됩니다. 시스템과 프로그램을 검사할 때 탐지된 취약점이 **시스템 취약점** 및 **취약한 프로그램** 탭의 같은 창에 표시됩니다.

보안위협을 검색할 경우 결과에 대한 정보가 카스퍼스키 안티 바이러스의 리포트에 기록됩니다.

프로그램 설정 창의 **취약점 검사** 섹션에서 스케줄 시작을 설정하고 바이러스 검사 작업과 유사하게 취약점 검사 작업에 사용할 검사 대상 개체 목록을 생성합니다. 기본적으로 컴퓨터에 이미 설치된 프로그램이 검사 개체로 선택됩니다.

참조:

취약점 검사 작업 시작 93

작업 실행 바로가기 생성 94

검사할 개체 목록 생성 94

스케줄: 스케줄 생성 95

스케줄: 계정 지정 95

취약점 검사 작업 시작

취약점 검사 작업을 시작하는 방법은 다음과 같습니다:

- 카스퍼스키 안티 바이러스 메인 창.
- 이전에 만든 바로가기 사용.

작업 실행 정보가 카스퍼스키 안티 바이러스 메인 창 및 **취약점 검사** 창에 표시됩니다.

- *바로가기를 사용하여 작업을 시작하려면 다음과 같이 하십시오:*

  1. 바로가기가 만들어진 폴더를 엽니다.
  2. 바로가기를 두 번 눌러 작업을 시작합니다. 메인 프로그램 창에 작업 진행 상태가 표시됩니다.

- *프로그램 창에서 취약점 검사 작업을 시작하려면 다음과 같이 하십시오:*

  1. 메인 프로그램 창을 엽니다.
  2. 창 왼쪽에서 **수동 검사** 섹션을 선택합니다.
  3. **취약점 검사 창 열기** 버튼을 누릅니다.

4. 취약점 검사 창이 열리면 **취약점 검사 시작** 버튼을 누릅니다. 작업 실행 과정이 **완료 예상 시간** 필드에 표시됩니다. 버튼을 다시 눌러 작업 실행을 중지합니다.

작업 실행 바로가기 생성

취약점 검사 작업을 빠르게 실행하도록 바로가기를 생성할 수 있습니다. 그러면 메인 프로그램 창을 열지 않고도 작업을 실행할 수 있습니다.

- *취약점 검사 작업을 실행하는 바로가기를 생성하려면 다음과 같이 하십시오:*

1. 메인 프로그램 창을 열고 창 상단의 **설정** 링크를 누릅니다.
2. 창 왼쪽에서 **수동 검사** 섹션을 선택합니다.
3. 창 오른쪽 부분의 **수동 검사 작업 바로가기** 섹션에서 작업 이름(**취약점 검사**) 옆에 있는 **바로가기 만들기** 버튼을 누릅니다.
4. 열리는 창에서 바로가기를 저장할 경로와 이름을 지정합니다. 기본적으로 바로가기는 현재 컴퓨터 사용자의 *My Computer* 폴더에 작업 이름으로 생성됩니다.

검사할 개체 목록 생성

취약점 검사 작업에는 검사할 개체에 대한 자체 기본 목록이 있습니다. 이러한 개체에는 컴퓨터에 설치된 운영 체제 및 프로그램이 포함됩니다. 여기에 컴퓨터 파일 시스템 개체(예: 논리 드라이브, **이메일 데이터베이스**) 또는 기타 유형의 개체(예: 네트워크 드라이브)와 같은 추가 개체를 검사하도록 지정할 수 있습니다.

개체를 추가하면 즉시 목록에 표시됩니다. 개체를 추가할 때 ☑ **하위 폴더 포함** 상자가 선택된 경우 반복해서 검사를 실행합니다. 수동으로 추가한 개체에 대해서도 바이러스가 검사됩니다.

목록에서 개체를 삭제하려면 개체를 선택하고 **삭제** 링크를 누릅니다.

기본적으로 목록에 표시되는 개체는 편집 또는 삭제할 수 없습니다.

목록에서 개체를 삭제할 뿐 아니라 검사 실행 시 일시적으로 건너뛸 수도 있습니다. 이렇게 하려면 목록에서 개체를 선택하고 개체 이름 왼쪽에 있는 상자를 체크해제합니다.

선택한 개체가 없이 검사 영역이 비어 있는 경우 검사 작업을 시작할 수 없습니다!

- *취약점 검사 작업 대상 개체 목록을 생성하려면 다음과 같이 하십시오.*

1. 메인 프로그램 창을 열고 창 상단의 **설정** 링크를 누릅니다.
2. 창 왼쪽의 **수동 검사** 섹션에서 **취약점 검사**를 선택합니다.
3. **검사 영역** 블록에서 선택한 작업에 대해 **설정** 버튼을 누릅니다.

4. 열리는 **취약점 검사: 개체 목록** 창에서 **추가, 편집, 삭제** 링크를 사용하여 목록을 생성합니다. 검사 대상 개체 목록에서 개체를 일시적으로 제외시키려면 해당 개체 옆에 있는 상자를 체크해제합니다.

스케줄: 스케줄 생성

취약점 검사 작업이 자동으로 실행되도록 스케줄을 지정할 수 있습니다.

이를 위해 작업 시작 간격을 적절하게 선택해야 합니다.
컴퓨터의 전원이 켜져 있지 않는 등 다양한 이유로 작업을 시작할 수 없는 경우 컴퓨터의 전원이 켜지면 자동으로 시작하도록 작업을 구성할 수 있습니다.

- *검사 작업 스케줄을 편집하려면 다음과 같이 하십시오:*

  1. 메인 프로그램 창을 열고 창 상단의 **설정** 링크를 누릅니다.
  2. 창 왼쪽의 **수동 검사** 섹션에서 **취약점 검사**를 선택합니다.
  3. **스케줄** 섹션에서 선택한 작업에 대해 **설정** 버튼을 누릅니다.
  4. 검사 작업을 가장 편리한 시간에 시작하려면 열리는 창의 **스케줄** 탭, **스케줄** 섹션에서 **수동 시작** 옵션을 선택합니다. 정기적으로 수행하려면 **스케줄 시작**을 선택하고 작업 실행 스케줄을 생성합니다.

- *건너뛴 작업이 자동으로 실행되도록 구성하려면 다음과 같이 하십시오:*

  1. 메인 프로그램 창을 열고 창 상단의 **설정** 링크를 누릅니다.
  2. 창 왼쪽의 **수동 검사** 섹션에서 **취약점 검사**를 선택합니다.
  3. **스케줄** 섹션에서 선택한 작업에 대해 **설정** 버튼을 누릅니다.
  4. 열리는 창의 **스케줄** 탭 아래 있는 **스케줄** 섹션에서 ☑ **건너뛴 작업 실행** 상자를 체크합니다.

스케줄: 계정 지정

카스퍼스키 안티 바이러스에서 취약점 검사를 수행할 때 사용할 계정을 지정할 수 있습니다.

- *계정을 지정하려면 다음과 같이 하십시오:*

  1. 메인 프로그램 창을 열고 창 상단의 **설정** 링크를 누릅니다.
  2. 창 왼쪽의 **수동 검사** 섹션에서 **취약점 검사**를 선택합니다.
  3. **스케줄** 섹션에서 선택한 작업에 대해 **설정** 버튼을 누릅니다.
  4. 열리는 창의 **스케줄** 탭 아래 있는 **사용자 계정** 섹션에서 ☑ **다음 계정으로 작업 실행** 상자를 체크하고 사용자 이름 및 암호를 지정합니다.

업데이트

컴퓨터를 확실하게 보호하려면 카스퍼스키 안티 바이러스를 최신 상태로 유지해야 합니다. 날마다 새로운 바이러스, 트로이목마, 악성 소프트웨어가 출현하기 때문에 카스퍼스키 안티 바이러스를 정기적으로 업데이트해야 중요한 데이터를 제대로 보호할 수 있습니다. 보안위협 및 처리 방법에 대한 정보는 카스퍼스키 안티 바이러스 데이터베이스에 저장되어 있으므로 이 데이터베이스를 적시에 업데이트하는 것이 필수입니다.

카스퍼스키 안티 바이러스 업데이트 시에는 다음 업데이트가 컴퓨터에 다운로드되어 설치됩니다:

- 카스퍼스키 안티 바이러스 데이터베이스.

  보안위협 및 네트워크 공격 시그니처와 처리 방법이 포함된 데이터베이스를 사용하여 정보가 보호됩니다. 실시간 감시 구성요소는 이 데이터베이스를 사용하여 컴퓨터에서 위험한 개체를 검색하여 치료합니다. 시시각각 신종 보안위협 레코드가 데이터베이스에 추가되므로 데이터베이스를 정기적으로 업데이트할 것을 권장합니다.

  카스퍼스키 안티 바이러스 데이터베이스 외에도 프로그램 구성요소가 네트워크 트래픽을 가로챌 수 있도록 하는 네트워크 드라이버가 업데이트됩니다.

- 프로그램 모듈.

  카스퍼스키 안티 바이러스 데이터베이스 외에도 프로그램 모듈을 업데이트할 수 있습니다. 업데이트 패키지는 카스퍼스키 안티 바이러스의 취약점을 수정하고 기존 기능을 강화 또는 개선합니다.

카스퍼스키 안티 바이러스의 주요 업데이트 경로는 특별한 카스퍼스키 랩 업데이트 서버입니다.

서버에서 업데이트를 성공적으로 다운로드하려면 컴퓨터를 인터넷에 연결해야 합니다. 기본적으로 인터넷 연결 설정은 자동으로 결정됩니다. 프록시 서버 설정이 자동으로 적절하게 구성되지 않는 경우 연결 설정을 수동으로 구성할 수 있습니다.

업데이트 시에는 컴퓨터에 있는 카스퍼스키 안티 바이러스 프로그램 모듈 및 데이터베이스가 업데이트 경로에 있는 것과 비교됩니다. 컴퓨터에 있는 프로그램 모듈 및 데이터베이스가 최신인 경우 컴퓨터 보호가 최신 상태라는 알림 창이 표시됩니다. 한편 컴퓨터에 있는 프로그램 모듈 및 데이터베이스가 업데이트 서버에 있는 것과 다를 경우 업데이트에서 변경된 부분만 다운로드합니다. 전체 데이터베이스와 프로그램 모듈이 다운로드되지 않기 때문에 파일 복사 속도가 빠르고 인터넷 트래픽이 적게 사용됩니다.

데이터베이스가 매우 오래된 경우 업데이트 패키지가 커서 인터넷 트래픽이 최대 수십 MB까지 증가할 수 있습니다.

카스퍼스키 안티 바이러스는 데이터베이스를 업데이트하기 전에 이전 버전의 데이터베이스로 롤백할 경우를 대비하여 백업 복사본을 생성합니다.

예를 들어 업데이트 과정에서 데이터베이스가 손상된 경우 업데이트 롤백 옵션이 필요할 수 있습니다. 이전 버전으로 간편하게 롤백하여 데이터베이스를 다시 업데이트할 수 있습니다.

카스퍼스키 안티 바이러스 업데이트 중에 로컬 경로로 가져온 업데이트를 배포할 수 있습니다. 이를 통해 네트워크 컴퓨터에서 데이터베이스 및 프로그램 모듈을 업데이트할 때 인터넷 트래픽을 줄일 수 있습니다.

또한 자동 업데이트 시작을 구성할 수도 있습니다.

메인 프로그램 창의 **업데이트 센터** 섹션에는 카스퍼스키 안티 바이러스 데이터베이스의 현재 상태에 대한 다음 정보가 표시됩니다:

- 배포 날짜 및 시간;
- 데이터베이스 레코드 수 및 구성;
- 데이터베이스 상태(최신, 오래됨, 손상).

업데이트 리포트(창 상단의 **리포트** 링크)를 통해 업데이트 작업 실행 중 발생한 이벤트에 대한 완전한 정보를 확인할 수 있습니다. 또한 **실시간 업데이트 상황 보기** 링크를 눌러 카스퍼스키 랩 웹사이트에서 실시간 업데이트 상황을 확인할 수 있습니다.

참조:

업데이트 시작 97

마지막으로 성공한 업데이트로 롤백 98

업데이트 경로 선택 98

프록시 서버 사용 99

지역 설정 100

업데이트 후 수행할 처리 방법 100

로컬 폴더에서 업데이트 101

업데이트 작업 스케줄 변경 101

다른 사용자 계정으로 업데이트 실행 102

업데이트 시작

업데이트는 언제든지 시작할 수 있습니다. 업데이트는 선택한 업데이트 경로에서 다운로드됩니다.

카스퍼스키 안티 바이러스를 업데이트하는 데는 다음 두 가지 방법 중 하나를 사용할 수 있습니다:

- 마우스 오른쪽 메뉴 사용
- 메인 프로그램 창 사용

업데이트 정보는 메인 프로그램 창의 **업데이트 센터** 섹션에 표시됩니다.

- *마우스 오른쪽 메뉴에서 카스퍼스키 안티 바이러스 업데이트를 시작하는 방법은 다음과 같습니다:*

  1. 작업 표시줄 알림 영역에서 프로그램 아이콘을 마우스 오른쪽 버튼으로 누릅니다.
  2. 드롭다운 메뉴에서 **업데이트** 항목을 선택합니다.

- *메인 프로그램 창에서 카스퍼스키 안티 바이러스 업데이트를 시작하는 방법은 다음과 같습니다:*

  1. 메인 프로그램 창을 엽니다.
  2. 창 왼쪽에서 **업데이트 센터** 섹션을 선택합니다.
  3. **업데이트 시작** 버튼을 누릅니다. 메인 프로그램 창에 작업 진행률이 표시됩니다.

마지막으로 성공한 업데이트로 롤백

업데이트 시작 시 카스퍼스키 안티 바이러스는 현재 데이터베이스 및 프로그램 모듈의 백업 복사본을 생성합니다. 이를 통해 업데이트에 실패하는 경우에도 이전 데이터베이스를 사용하여 카스퍼스키 안티 바이러스를 계속 작동할 수 있습니다.

롤백 옵션은 데이터베이스의 일부가 손상된 경우 유용합니다. 로컬 데이터베이스는 사용자 또는 악성 프로그램에 의해 손상될 수 있습니다. 하지만 이는 카스퍼스키 안티 바이러스 자기-보호를 중지한 경우에만 발생합니다. 이전 버전으로 간편하게 롤백하여 데이터베이스를 이후에 업데이트할 수 있습니다.

- *이전 데이터베이스 버전으로 롤백하는 방법은 다음과 같습니다:*

  1. 메인 프로그램 창을 엽니다.
  2. 창 왼쪽에서 **업데이트 센터** 섹션을 선택합니다.
  3. **이전 데이터베이스로 롤백** 버튼을 누릅니다.

업데이트 경로 선택

*업데이트 경로*는 카스퍼스키 안티 바이러스의 데이터베이스 및 프로그램 모듈 업데이트가 포함된 리소스입니다. 업데이트 경로는 HTTP 또는 FTP 서버이거나 로컬 또는 네트워크 폴더가 될 수 있습니다.

주요 업데이트 경로는 카스퍼스키 랩의 업데이트 서버입니다. 이것은 모든 카스퍼스키 랩 제품의 데이터베이스 및 프로그램 모듈 업데이트가 포함된 특별한 웹사이트입니다.

카스퍼스키 랩의 업데이트 서버에 접근할 수 없는 경우(예: 컴퓨터에 인터넷이 연결되지 않음) 카스퍼스키 랩 한국 지사(02-508-8773)에 연락하여 카스퍼스키 랩 파트너 연락처 정보를 요청할 수 있습니다. 카스퍼스키 랩 파트너가 업데이트를 플로피 디스크 또는 압축 디스크에 제공할 수 있습니다.

이동식 디스크에 있는 업데이트를 복사하여 FTP 또는 HTTP 사이트에 업로드하거나 로컬 또는 네트워크 폴더에 저장할 수 있습니다.

이동식 장치에 담긴 업데이트를 주문할 때는 프로그램 모듈에 대한 업데이트도 필요한지 알려 주십시오.

기본적으로 업데이트 경로 목록에는 카스퍼스키 랩의 업데이트 서버만 포함되어 있습니다.

업데이트 경로로 LAN 외부 리소스를 선택한 경우 업데이트를 위해 인터넷 연결이 필요합니다.

여러 리소스를 업데이트 경로로 선택한 경우 카스퍼스키 안티 바이러스는 목록 위부터 아래 순서로 하나씩 연결해 보고 가장 먼저 가능한 경로에서 업데이트를 가져옵니다.

- *업데이트 경로를 선택하는 방법은 다음과 같습니다:*

  1. 메인 프로그램 창을 열고 창 상단의 **설정** 링크를 누릅니다.
  2. 창 왼쪽에서 **업데이트 센터** 섹션을 선택합니다.
  3. **업데이트 경로** 섹션에서 **설정** 버튼을 누릅니다.
  4. 열리는 창의 **경로** 탭에서 **추가** 링크를 누릅니다.
  5. 열리는 **업데이트 경로 선택** 창에서 FTP 또는 HTTP 사이트를 선택하거나 IP 주소, 심볼 이름 또는 URL 을 입력합니다.

프록시 서버 사용

프록시 서버를 사용하여 인터넷에 연결하는 경우 프록시 설정을 구성해야 합니다.

- *프록시 서버를 구성하는 방법은 다음과 같습니다:*

  1. 메인 프로그램 창을 열고 창 상단의 **설정** 링크를 누릅니다.
  2. 창 왼쪽에서 **업데이트 센터** 섹션을 선택합니다.
  3. **업데이트 경로** 섹션에서 **설정** 버튼을 누릅니다.
  4. 열리는 창의 **경로** 탭에서 **프록시 서버** 버튼을 누릅니다.
  5. 열리는 프록시 서버 설정 창에서 **프록시 서버 설정**을 구성합니다.

지역 설정

업데이트 경로로 카스퍼스키 랩 업데이트 서버를 사용하는 경우 업데이트를 다운로드할 때 최적의 서버 위치를 선택할 수 있습니다. 카스퍼스키 랩 서버는 여러 국가에 있습니다. 해당 위치에서 가장 가까운 카스퍼스키 랩 업데이트 서버를 선택하면 시간을 절약하고 업데이트를 더욱 빠르게 다운로드할 수 있습니다.

- *가장 가까운 서버를 선택하는 방법은 다음과 같습니다:*

  1. 메인 프로그램 창을 열고 창 상단의 **설정** 링크를 누릅니다.
  2. 창 왼쪽에서 **업데이트 센터** 섹션을 선택합니다.
  3. **업데이트 경로** 섹션에서 **설정** 버튼을 누릅니다.
  4. 열리는 창의 **경로** 탭, **지역 설정** 섹션에서 **목록에서 선택** 상자를 체크한 다음 드롭다운 목록에서 현재 위치와 가장 가까운 국가를 선택합니다.

     자동 탐지 옵션을 선택하는 경우 업데이트 시 운영 체제 레지스트리에서 해당 위치에 대한 정보가 복사됩니다.

업데이트 후 수행할 처리 방법

카스퍼스키 안티 바이러스에서는 업데이트 후 자동으로 수행할 처리 방법을 지정할 수 있습니다. 다음과 같은 처리 방법을 사용할 수 있습니다:

- **격리저장소 다시 검사**. 격리저장소 구역에는 카스퍼스키 안티 바이러스에서 감염의심 또는 감염 위험이 있는 것으로 파악된 개체가 포함되어 있습니다. 데이터베이스 업데이트 후에는 보안위협이 더욱 명확하게 확인되어 처리할 수 있는 가능성이 있습니다. 따라서 카스퍼스키 안티 바이러스는 매번 업데이트 후 격리저장소 개체를 검사합니다. 검사를 통해 격리저장소 개체의 상태가 변경될 수 있습니다. 그에 따라 일부 개체는 이전 위치로 복원되어 정상적으로 사용할 수 있습니다.
- **폴더로 업데이트 파일 복사**. 컴퓨터가 홈 LAN 에 연결된 경우 각 컴퓨터에 개별적으로 업데이트를 다운로드하여 설치할 필요가 없습니다. 업데이트 배포 서비스를 사용하여 네트워크 대역폭을 저장할 수 있습니다. 업데이트 배포 서비스는 업데이트가 한 번만 다운로드되도록 보장합니다.

- *업데이트 후 격리저장소 파일을 검사하는 방법은 다음과 같습니다:*

  1. 메인 프로그램 창을 열고 창 상단의 **설정** 링크를 누릅니다.
  2. 창 왼쪽에서 **업데이트 센터** 섹션을 선택합니다.
  3. 고급 섹션에서 업데이트 후 격리저장소 다시 검사 상자를 체크합니다.

로컬 폴더에서 업데이트

로컬 폴더에서 업데이트를 가져오는 절차는 다음과 같습니다:

1. 네트워크에 있는 컴퓨터 중 하나가 카스퍼스키 랩 업데이트 서버 또는 최신 업데이트를 호스팅하는 미러 서버에서 카스퍼스키 안티 바이러스 업데이트 패키지를 가져옵니다. 가져온 업데이트가 공유 폴더에 배치됩니다.

2. 네트워크에 있는 다른 컴퓨터들이 공용 접근 폴더에 접근하여 카스퍼스키 안티 바이러스 업데이트를 가져옵니다.

- *업데이트 배포 모드를 작동하는 방법은 다음과 같습니다:*

1. 메인 프로그램 창을 열고 창 상단의 **설정** 링크를 누릅니다.

2. 창 왼쪽에서 **업데이트 센터** 섹션을 선택합니다.

3. **고급** 섹션에서 ☑ **폴더로 업데이트 파일 복사** 상자를 체크하고 아래 칸에 다운로드한 모든 업데이트를 복사할 공용 폴더 경로를 지정합니다. 또한 **찾아보기** 버튼을 누른 후 표시되는 창에서 경로를 선택할 수도 있습니다.

- *네트워크에 있는 모든 컴퓨터에 대해 선택한 공용 접근 폴더에서 업데이트를 수행하는 방법은 다음과 같습니다:*

1. 메인 프로그램 창을 열고 창 상단의 **설정** 링크를 누릅니다.

2. 창 왼쪽에서 **업데이트 센터** 섹션을 선택합니다.

3. **업데이트 경로** 섹션에서 **설정** 버튼을 누릅니다.

4. 열리는 창의 **경로** 탭에서 **추가** 링크를 누릅니다.

5. 열리는 **업데이트 경로 선택** 창에서 폴더를 선택하거나 경로 칸에 폴더의 전체 경로를 입력합니다.

6. 경로 탭에서 ☑ **카스퍼스키 랩 업데이트 서버** 상자를 체크해제합니다.

업데이트 작업 스케줄 변경

카스퍼스키 안티 바이러스 업데이트 작업의 시작 모드는 카스퍼스키 안티 바이러스 구성 마법사에서 선택합니다. 선택한 업데이트 시작 모드를 변경하려면 다시 구성하면 됩니다.

업데이트 작업은 다음 모드 중 하나를 사용하여 실행할 수 있습니다:

- ◉ **자동 실행**. 카스퍼스키 안티 바이러스가 지정된 간격으로 업데이트 경로에서 업데이트가 있는지 확인합니다. 검사 빈도는 안티 바이러스 급증 시 늘어날 수 있고 반대의 경우 줄어들 수 있습니다. 새 업데이트가 발견되면 컴퓨터에 다운로드하여 설치합니다.

- **스케줄 시작**. (시간 간격은 설정에 따라 달라짐). 생성된 스케줄에 따라 업데이트가 자동으로 실행됩니다.
- **수동 실행**. 이 옵션을 선택할 경우 카스퍼스키 안티 바이러스 업데이트를 수동으로 실행해야 합니다.

- *업데이트 작업 실행 스케줄을 구성하는 방법은 다음과 같습니다:*

1. 메인 프로그램 창을 열고 창 상단의 **설정** 링크를 누릅니다.
2. 창 왼쪽에서 **업데이트 센터** 섹션을 선택합니다.
3. **스케줄** 섹션에서 **설정** 버튼을 누릅니다.
4. 열리는 창의 **스케줄** 탭, **스케줄** 섹션에서 업데이트 작업 시작 모드를 선택합니다. **스케줄 시작** 옵션을 선택한 경우 스케줄을 생성합니다.

   컴퓨터의 전원이 켜져 있지 않는 등 다양한 이유로, 가능할 때 최대한 빨리 자동으로 작업을 시작하도록 구성할 수 있습니다. 이렇게 하려면 창 하단에서 **건너뛴 작업 실행** 상자를 체크합니다. **시**, **분** 및 **프로그램 시작 후**를 제외한 모든 스케줄 옵션에 이 체크상자가 표시됩니다.

다른 사용자 계정으로 업데이트 실행

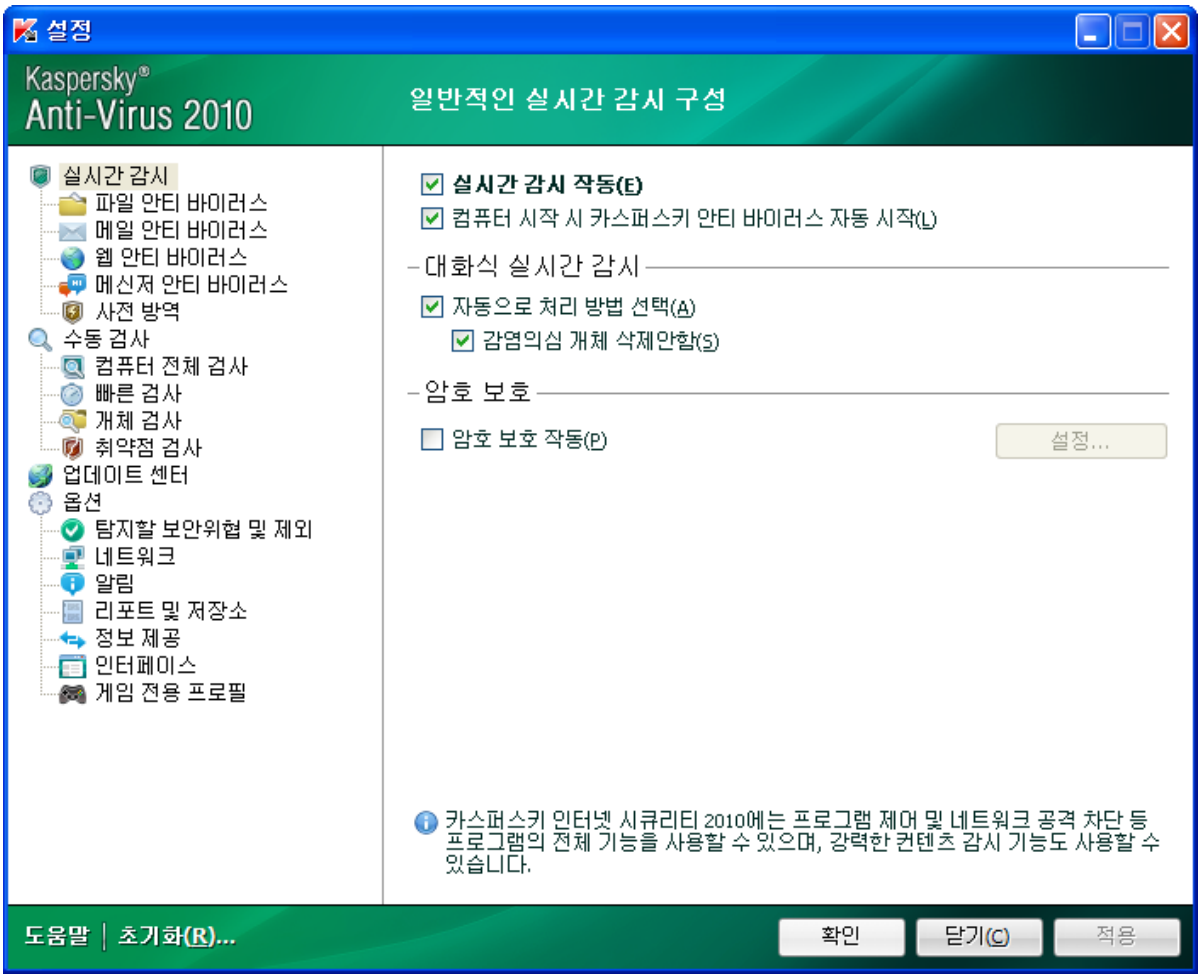
기본적으로 업데이트 절차는 시스템 계정으로 실행됩니다. 그러나 카스퍼스키 안티 바이러스는 사용자에게 접근 권한이 없는 경로(예: 업데이트가 포함된 네트워크 폴더) 또는 인증된 프록시 사용자 자격 증명이 없는 경로에서도 업데이트할 수 있습니다. 해당 권한이 있는 사용자 계정을 대신해서 카스퍼스키 안티 바이러스를 실행할 수 있습니다.

- *다른 사용자 계정으로 업데이트를 시작하는 방법은 다음과 같습니다:*

1. 메인 프로그램 창을 열고 창 상단의 **설정** 링크를 누릅니다.
2. 창 왼쪽에서 **업데이트 센터** 섹션을 선택합니다.
3. **스케줄** 섹션에서 **설정** 버튼을 누릅니다.
4. 열리는 창의 스케줄 탭 아래 있는 사용자 계정 섹션에서 다음 계정으로 작업 실행 상자를 체크하고 사용자 이름 및 암호를 지정합니다.

프로그램 설정 구성

프로그램 설정 창을 사용하면 주요 카스퍼스키 안티 바이러스 설정에 빠르게 접근할 수 있습니다.



프로그램 설정 구성 창

프로그램 설정 창은 두 부분으로 구성됩니다:

- 창 왼쪽 부분에서는 카스퍼스키 안티 바이러스 구성요소, 바이러스 검사 작업, 업데이트 작업 등에 접근할 수 있습니다.
- 창 오른쪽 부분에는 창 왼쪽 부분에서 선택한 구성요소, 작업 등에 대한 설정 목록이 표시됩니다.

이 창은 다음 방법으로 열 수 있습니다:

- 메인 프로그램 창에서 열 경우. 메인 창 상단에 있는 **설정** 링크를 누릅니다.

- 마우스 오른쪽 메뉴에서 열 경우. 프로그램의 마우스 오른쪽 메뉴에서 **설정** 항목을 선택합니다.

마우스 오른쪽 메뉴

참조:

실시간 감시 104
파일 안티 바이러스 107
메일 안티 바이러스 108
웹 안티 바이러스 108
메신저 안티 바이러스 109
사전 방역 110
검사 110
업데이트 111
설정 112

실시간 감시

실시간 감시 창에서 다음과 같은 카스퍼스키 안티 바이러스 추가 기능을 사용할 수 있습니다:

- 카스퍼스키 안티 바이러스 실시간 감시 작동/중지
- 시스템 시작 시 카스퍼스키 안티 바이러스 자동 실행
- 대화식 실시간 감시 모드 사용
- 카스퍼스키 안티 바이러스 접근 제한.

실시간 감시 작동/중지

운영 체제가 로딩되면 기본적으로 카스퍼스키 안티 바이러스가 실행되어(끄지 않는 한) 컴퓨터를 보호합니다. 모든 실시간 감시 구성요소가 실행됩니다.

카스퍼스키 안티 바이러스에서 제공한 실시간 감시를 전부 또는 일부 중지할 수 있습니다.

카스퍼스키 랩 전문가들은 컴퓨터 감염 및 데이터 손실이 발생할 수 있기 때문에 **실시간 감시를 중지하지 않을 것**을 강력히 권장합니다.

실시간 감시를 중지할 경우 모든 구성요소가 중지됩니다. 이는 다음을 통해 확인할 수 있습니다:

- 작업 표시줄 알림 영역의 카스퍼스키 안티 바이러스 아이콘이 중지됨(회색)
- 보안 표시기가 빨강색.

여기서 실시간 감시 중지는 실시간 감시 구성요소가 중지된다는 의미이며, 실시간 감시 구성요소를 중지하거나 일시 중지해도 바이러스 검사 작업 성능과 카스퍼스키 인터넷 보안 업데이트에는 영향이 없습니다.

- *실시간 감시를 완전히 중지하려면 다음과 같이 하십시오:*

  1. 메인 프로그램 창을 열고 창 상단의 **설정** 링크를 누릅니다.
  2. 열리는 창에서 **실시간 감시** 섹션을 선택합니다.
  3. ☑ **실시간 감시 작동** 상자를 체크해제합니다.

시스템 시작 시 카스퍼스키 안티 바이러스 실행

특정한 이유로 카스퍼스키 안티 바이러스를 완전히 중지해야 하는 경우 카스퍼스키 안티 바이러스의 마우스 오른쪽 메뉴에서 **종료** 항목을 선택합니다. 그러면 카스퍼스키 안티 바이러스 프로그램이 RAM 에서 언로드되고 컴퓨터가 보호되지 않는 상태로 실행됩니다.

시작 → **프로그램** → **카스퍼스키 안티 바이러스 2010** → **카스퍼스키 안티 바이러스 2010** 프로그램 메뉴에서 카스퍼스키 안티 바이러스를 시작하여 컴퓨터의 실시간 감시를 작동할 수 있습니다.

또한 운영 체제를 다시 시작한 후 실시간 감시를 자동으로 다시 작동할 수도 있습니다.

- *이 모드를 작동하려면 다음과 같이 하십시오:*

  1. 메인 프로그램 창을 열고 창 상단의 **설정** 링크를 누릅니다.
  2. 열리는 창에서 **실시간 감시** 섹션을 선택합니다.
  3. ☑ **컴퓨터 시작 시 카스퍼스키 안티 바이러스 자동 시작** 상자를 체크합니다.

대화식 실시간 감시 모드 사용

카스퍼스키 안티 바이러스는 두 가지 모드를 통해 사용자와 상호 작용합니다:

- *대화식 실시간 감시 모드.* 카스퍼스키 안티 바이러스가 사용자에게 위험하거나 의심스러운 모든 이벤트를 알립니다. 이 모드에서는 사용자가 작업을 허락할지 차단할지를 독립적으로 결정할 수 있습니다.
- *자동 실시간 감시 모드.* 카스퍼스키 안티 바이러스가 위험한 이벤트에 대응하여 카스퍼스 랩에서 권장하는 처리 방법을 자동으로 적용합니다.

- *자동 실시간 감시 모드를 사용하려면 다음과 같이 하십시오:*

1. 메인 프로그램 창을 열고 창 상단의 **설정** 링크를 누릅니다.
2. 열리는 창에서 **실시간 감시** 섹션을 선택합니다.
3. **대화식 실시간 감시** 섹션에서 ☑ **자동으로 처리 방법 선택** 상자를 체크합니다. 자동 모드로 실행 시 카스퍼스키 안티 바이러스가 감염의심 개체를 삭제하지 않길 원하는 경우 ☑ **감염의심 개체 삭제안함** 상자를 체크합니다.

카스퍼스키 안티 바이러스 접근 제한

개인 컴퓨터는 컴퓨터 활용 능력이 각기 다른 사람들을 비롯해 여러 사람이 사용할 수 있습니다. 따라서 카스퍼스키 안티 바이러스와 설정에 대한 액세스를 열어 둘 경우 컴퓨터의 보안 레벨이 전체적으로 크게 낮아질 수 있습니다.

컴퓨터의 보안 레벨을 높이려면 암호를 사용하여 카스퍼스키 안티 바이러스에 액세스하십시오. 위험 개체 탐지 알림을 제외한 카스퍼스키 안티 바이러스 작동을 차단하고 다음과 같은 작업이 수행되는 것을 방지할 수 있습니다.

- 프로그램 설정 변경
- 프로그램 종료.

- *암호를 사용하여 카스퍼스키 안티 바이러스에 대한 액세스를 감시하려면 다음과 같이 하십시오.*

1. 메인 프로그램 창을 열고 창 상단의 **설정** 링크를 누릅니다.
2. 열리는 창에서 **실시간 감시** 섹션을 선택합니다.
3. **암호 보호** 섹션에서 ☑ **암호 보호 작동** 상자를 체크하고 **설정** 버튼을 누릅니다.
4. **암호 보호** 창이 열리면 암호를 입력하고 접근 제한을 적용할 영역을 지정합니다. 이제 컴퓨터 사용자가 선택한 작업을 수행하려고 시도할 때마다 카스퍼스키 안티 바이러스가 항상 암호 입력을 요청하게 됩니다.

파일 안티 바이러스

파일 안티 바이러스 구성요소 설정이 창에 그룹화되어 있습니다. 설정을 편집하여 다음 처리 방법을 수행할 수 있습니다:

- 파일 안티 바이러스 중지
- 보안 레벨 변경
- 탐지된 개체에 수행할 처리 방법 변경
- 실시간 감시 영역 생성
- 감시 최적화
- 복합 파일 검사 구성
- 감시 방식 변경
- 휴리스틱 분석기 사용
- 구성요소 일시 중지
- 고급 감시 기술 선택
- 기본 실시간 감시 설정 복원(변경된 경우).

- *파일 안티 바이러스를 중지하려면 다음과 같이 하십시오.*

  1. 메인 프로그램 창을 열고 창 상단의 **설정** 링크를 누릅니다.
  2. 열리는 창의 **실시간 감시** 섹션에서 **파일 안티 바이러스** 구성요소를 선택합니다.
  3. 창 오른쪽에 있는 ☑ **파일 안티 바이러스 작동** 상자를 체크해제합니다.

- *파일 안티 바이러스 설정을 계속 진행하려면 다음과 같이 하십시오.*

  1. 메인 프로그램 창을 열고 창 상단의 **설정** 링크를 누릅니다.
  2. 열리는 창의 **실시간 감시** 섹션에서 **파일 안티 바이러스** 구성요소를 선택합니다.
  3. 창 오른쪽에서 보안위협에 대한 보안 레벨 및 처리에 대한 구성요소 설정을 선택합니다. 다른 파일 안티 바이러스 설정으로 전환하려면 **설정** 버튼을 누릅니다.

메일 안티 바이러스

메일 안티 바이러스 구성요소 설정이 창에 그룹화되어 있습니다. 설정을 편집하여 다음 처리 방법을 수행할 수 있습니다.

- 메일 안티 바이러스 중지
- 보안 레벨 변경
- 탐지된 개체에 수행할 처리 방법 변경
- 실시간 감시 영역 생성
- 휴리스틱 분석기 사용
- 복합 파일 검사 구성
- 이메일 메시지에 첨부되는 개체의 필터링 조건 구성
- 기본 이메일 실시간 감시 설정 복원.

- *메일 안티 바이러스를 중지하려면 다음과 같이 하십시오.*

  1. 메인 프로그램 창을 열고 창 상단의 **설정** 링크를 누릅니다.
  2. 열리는 창의 **실시간 감시** 섹션에서 **메일 안티 바이러스** 구성요소를 선택합니다.
  3. 창 오른쪽에 있는 ☑ **메일 안티 바이러스 작동** 상자를 체크해제합니다.

- *메일 안티 바이러스 설정을 계속 진행하려면 다음과 같이 하십시오.*

  1. 메인 프로그램 창을 열고 창 상단의 **설정** 링크를 누릅니다.
  2. 열리는 창의 **실시간 감시** 섹션에서 **메일 안티 바이러스** 구성요소를 선택합니다.
  3. 창 오른쪽에서 보안위협에 대한 보안 레벨 및 처리에 대한 구성요소 설정을 선택합니다. 다른 메일 안티 바이러스 설정으로 전환하려면 **설정** 버튼을 누릅니다.

웹 안티 바이러스

웹 안티 바이러스 구성요소 설정이 창에 그룹화되어 있습니다. 설정을 편집하여 다음 처리 방법을 수행할 수 있습니다.

- 웹 안티 바이러스 중지
- 보안 레벨 변경

- 탐지된 개체에 수행할 처리 방법 변경
- 실시간 감시 영역 생성
- 감시 방법 변경
- URL 검사 모듈 사용
- 감시 최적화
- 휴리스틱 분석기 사용
- 기본 웹 안티 바이러스 설정 복원

- *웹 안티 바이러스를 중지하려면 다음과 같이 하십시오.*

  1. 메인 프로그램 창을 열고 창 상단의 **설정** 링크를 누릅니다.
  2. 열리는 창의 **실시간 감시** 섹션에서 **웹 안티 바이러스** 구성요소를 선택합니다.
  3. 창 오른쪽에 있는 ☐ **웹 안티 바이러스** 작동 상자를 체크 해제합니다**.**

- *웹 안티 바이러스 설정을 계속 진행하려면 다음과 같이 하십시오.*

  1. 메인 프로그램 창을 열고 창 상단의 **설정** 링크를 누릅니다.
  2. 열리는 창의 **실시간 감시** 섹션에서 **웹 안티 바이러스** 구성요소를 선택합니다.
  3. 창 오른쪽에서 보안위협에 대한 보안 레벨 및 처리에 대한 구성요소 설정을 선택합니다. 다른 웹 안티 바이러스 설정으로 전환하려면 **설정** 버튼을 누릅니다.

메신저 안티 바이러스

메신저 안티 바이러스 구성요소 설정이 창에 그룹화되어 있습니다. 설정을 편집하여 다음 처리 방법을 수행할 수 있습니다.

- 메신저 안티 바이러스 중지
- 실시간 감시 영역 생성
- 감시 방법 변경
- 휴리스틱 분석기 사용

- *메신저 안티 바이러스를 중지하려면 다음과 같이 하십시오.*

  1. 메인 프로그램 창을 열고 창 상단의 **설정** 링크를 누릅니다.

2. 열리는 창의 **실시간 감시** 섹션에서 **메신저 안티 바이러스** 구성요소를 선택합니다.

3. 창 오른쪽에 있는 ☑ **메신저 안티 바이러스 작동** 상자를 체크해제합니다.

- *메신저 안티 바이러스 설정을 계속 진행하려면 다음과 같이 하십시오.*

1. 메인 프로그램 창을 열고 창 상단의 **설정** 링크를 누릅니다.

2. 열리는 창의 **실시간 감시** 섹션에서 **메신저 안티 바이러스** 구성요소를 선택합니다.

3. 창 오른쪽에서 구성요소 설정의 필요한 사항을 변경합니다.

사전 방역

이 창은 사전 방역 구성요소의 설정을 그룹화합니다. 설정을 편집하여 다음 처리 방법을 수행할 수 있습니다:

- 사전 방역 중지
- 위험 활동 목록 관리
- 시스템에서 위험 활동에 대한 프로그램의 반응 변경
- 신뢰하는 프로그램 그룹 생성
- 시스템 사용자 계정 감시

- *사전 방역을 중지하려면 다음과 같이 하십시오:*

1. 메인 프로그램 창을 열고 창 상단의 **설정** 링크를 누릅니다.

2. 열리는 창의 **실시간 감시** 섹션에서 **사전 방역** 구성요소를 선택합니다.

3. 창 오른쪽에 있는 ☑ **사전 방역 사용** 상자를 체크해제합니다.

- *사전 방역 설정 편집을 계속 진행하려면 다음과 같이 하십시오:*

1. 메인 프로그램 창을 열고 창 상단의 **설정** 링크를 누릅니다.

2. 열리는 창의 **실시간 감시** 섹션에서 **사전 방역** 구성요소를 선택합니다.

3. 창 오른쪽에서 구성요소 설정의 필요한 사항을 변경합니다.

검사

각 작업에 할당된 속성 세트에 따라 컴퓨터의 개체를 검사하는 데 사용할 방법을 선택할 수 있습니다.

카스퍼스키 랩은 바이러스 검사 작업과 취약점 검사 작업을 구분합니다. 바이러스 검사 작업은 다음과 같습니다:

- **개체 검사**. 사용자가 선택한 개체를 검사합니다. 컴퓨터 파일 시스템의 모든 개체를 검사할 수 있습니다.
- **컴퓨터 전체 검사**. 전체 컴퓨터를 완전히 검사합니다. 기본적으로 시스템 메모리, 시작 시 로딩된 프로그램, 시스템 백업, 이메일 데이터베이스, 하드 드라이브, 이동식 저장 장치, 네트워크 드라이브 등은 검사 대상입니다.
- **빠른 검사**. 운영 체제 자동 시작 개체에 바이러스가 있는지 검사합니다.

각 바이러스 검사 작업의 설정 창에서 다음과 같은 작업을 수행할 수 있습니다:

- 런타임 시 작업 행동을 정의하는 관련 설정에 따라 보안 레벨 선택
- 프로그램이 감염 개체/감염 위험 개체를 탐지한 경우 적용할 처리 방법 선택
- 자동으로 실행할 작업의 스케줄 생성
- 검사 대상 개체 목록 생성(빠른 검사 및 컴퓨터 전체 검사의 경우)
- 바이러스를 검사할 감시 파일 형태 지정
- 복합 파일의 검사 설정 지정
- 검사 방법 및 기술 지정.

이동식 드라이브를 컴퓨터에 연결하면 **검사** 섹션에서 자동 이동식 드라이브 검사의 설정을 지정하고 바이러스 검사 및 취약점 검사 작업을 빠르게 시작할 수 있는 바로가기를 생성할 수 있습니다.

취약점 검사 작업의 설정 창에서 다음과 같은 작업을 수행할 수 있습니다:

- 자동으로 실행할 작업의 스케줄 생성
- 검사 대상 개체 목록 생성.

- *작업 설정을 편집하려면 다음과 같이 하십시오:*

1. 프로그램 설정 창을 엽니다.
2. 창 왼쪽의 **수동 검사**(**컴퓨터 전체 검사**, **빠른 검사**, **개체 검사**, **취약점 검사**) 섹션에서 필요한 작업을 선택합니다.
3. 창 오른쪽에서 설정을 구성합니다.

업데이트

카스퍼스키 안티 바이러스 업데이트는 파라미터 집합에 따라 수행됩니다.

업데이트 작업 구성 창에서는 다음 작업을 수행할 수 있습니다:

- 카스퍼스키 안티 바이러스 업데이트를 복사하고 설치할 리소스 주소 변경
- 카스퍼스키 안티 바이러스 업데이트 프로세스를 시작할 모드 유형 지정
- 작업 실행 스케줄 설정
- 업데이트를 시작할 계정 지정
- 카스퍼스키 안티 바이러스 업데이트 후 수행할 처리 방법 선택.

- *업데이트 구성을 처리하는 방법은 다음과 같습니다:*

1. 메인 프로그램 창을 열고 창 상단의 **설정** 링크를 누릅니다.
2. 창 왼쪽에서 **업데이트 센터** 섹션을 선택합니다.
3. 창 오른쪽 부분에서 필요한 스케줄을 선택하고 업데이트 경로를 선택합니다. **고급** 섹션에서 다른 작업 설정을 구성합니다.

설정

설정 창에서 다음과 같은 카스퍼스키 안티 바이러스 추가 기능을 사용할 수 있습니다:

- 카스퍼스키 안티 바이러스 자기 보호 기능
- 고급 치료 기술 사용
- 배터리 절약 서비스
- 다른 프로그램의 속도가 느려질 경우 바이러스 검사 작업 실행 연기
- 카스퍼스키 안티 바이러스 설정 내보내기/가져오기
- 카스퍼스키 안티 바이러스 기본 설정 복원.

카스퍼스키 안티 바이러스 자기-보호 기능

카스퍼스키 안티 바이러스는 악성 프로그램으로부터 컴퓨터 보안을 지키기 때문에 악성 프로그램의 공격 대상이 될 수 있습니다. 악성 프로그램은 카스퍼스키 안티 바이러스를 차단하거나 삭제하려 할 수 있습니다.

컴퓨터 보안 시스템의 신뢰성을 유지하기 위해 카스퍼스키 안티 바이러스에는 원격 접근으로부터의 자기-보호 및 보호 기능이 제공됩니다.

64비트 운영 체제 및 Microsoft Windows Vista를 실행하는 컴퓨터에서 카스퍼스키 안티 바이러스 자기-보호는 로컬 드라이브 및 시스템 레지스트리 레코드가 수정 또는 삭제되지 않도록 방지하는 데만 사용됩니다.

때때로 원격 접근 방지를 사용하는 동안 원격 관리 프로그램(예: RemoteAdmin)이 필요할 수 있습니다. 원격 접근 방지의 정상적인 성능을 위해 원격 관리 프로그램을 신뢰하는 프로그램 목록에 추가하고 **프로그램 활동 감시 안함** 옵션을 작동해야 합니다.

- *카스퍼스키 안티 바이러스 자기-보호 메커니즘을 작동하려면 다음과 같이 하십시오:*

  1. 메인 프로그램 창을 열고 창 상단의 **설정** 링크를 누릅니다.
  2. 열리는 창에서 **옵션** 섹션을 선택합니다.
  3. 하드 드라이브에 있는 자기-보호 파일, RAM 프로세스 및 시스템 레지스트리 레코드가 삭제 또는 수정되지 않도록 카스퍼스키 안티 바이러스 감시 메커니즘을 작동하려면 **자기-보호** 섹션에서 ☑ **자기-보호 작동** 상자를 체크합니다.

     원격으로 프로그램 서비스를 관리하려는 시도를 차단하려면 **자기-보호** 섹션에서 ☑ **외부 서비스 제어 중지** 상자를 체크합니다.

     위의 처리 방법 중 하나를 시도하면 작업 표시줄 알림 영역의 프로그램 아이콘 위에 메시지가 나타납니다(사용자가 알림 서비스를 중지하지 않은 경우).

고급 치료 기술

오늘날의 악성 프로그램은 운영 체제의 최하위 계층에 침입해서 삭제하기가 거의 불가능합니다. 시스템 내에서 악성 활동이 탐지되는 경우 카스퍼스키 안티 바이러스는 보안위협을 없애고 컴퓨터에서 삭제하도록 특별한 고급 치료 절차를 수행하도록 제안합니다.

이 절차가 끝나면 컴퓨터를 다시 시작해야 합니다. 컴퓨터를 다시 시작한 후에는 전체 바이러스 검사를 실행하는 것이 좋습니다.

- *고급 치료 절차를 시작하려면 다음과 같이 하십시오:*

  1. 메인 프로그램 창을 열고 창 상단의 **설정** 링크를 누릅니다.
  2. 열리는 창에서 **옵션** 섹션을 선택합니다.
  3. **효율성** 섹션에서 ☑ **고급 치료 기술 사용** 상자를 체크합니다.

랩탑에서 카스퍼스키 안티 바이러스 사용

휴대용 컴퓨터에서 전원을 절약하기 위해 바이러스 검사 작업을 연기할 수 있습니다.

바이러스 검사와 업데이트를 위해서는 모두 상당한 리소스와 시간이 소요되므로 이러한 작업의 스케줄된 시작을 중지하는 것이 좋습니다. 이렇게 하면 배터리 충전량을 절약할 수 있습니다. 필요할 때 언제든지 카스퍼스키 안티 바이러스를 업데이트하거나 바이러스 검사를 직접 시작할 수 있습니다.

- *배터리 절약 서비스를 사용하려면 다음과 같이 하십시오:*

  1. 메인 프로그램 창을 열고 창 상단의 **설정** 링크를 누릅니다.
  2. 열리는 창에서 **옵션** 섹션을 선택합니다.
  3. **효율성** 섹션에서 ☑ **배터리 전원으로 실행 중이면 스케줄된 검사 중지** 상자를 체크합니다.

작업 실행 중의 컴퓨터 성능

CPU(중앙 처리 장치) 및 디스크 저장소 하위 시스템에 대한 로드를 제한하기 위해 바이러스 검사 작업을 연기할 수 있습니다.

검사 작업을 실행하면 CPU 및 디스크 하위 시스템에 대한 로드가 증가하여 다른 프로그램이 느려질 수 있습니다. 그러한 상황이 발생할 경우 카스퍼스키 안티 바이러스는 기본적으로 바이러스 검사 작업을 중지하고 사용자 프로그램을 위해 시스템 리소스를 확보합니다.

그러나 CPU 리소스를 사용할 수 있게 되면 즉시 시작된 후 백그라운드에서 실행되는 프로그램도 몇 가지 있습니다. 그러한 프로그램의 성능을 위해 검사를 중지하고 시스템 리소스 우선권을 할당해서는 안 됩니다.

이 설정은 모든 검사 작업에 대해 개별적으로 구성할 수 있습니다. 이 경우 특정 작업에 대한 구성이 보다 높은 우선 순위를 갖습니다.

- *다른 프로그램이 느려지는 경우 검사 작업 실행을 연기하려면 다음과 같이 하십시오:*

  1. 메인 프로그램 창을 열고 창 상단의 **설정** 링크를 누릅니다.
  2. 열리는 창에서 **옵션** 섹션을 선택합니다.
  3. **효율성** 섹션에서 ☑ **다른 프로그램에 컴퓨터 리소스 우선권 할당** 상자를 체크합니다.

카스퍼스키 안티 바이러스 설정 내보내기/가져오기

카스퍼스키 안티 바이러스에서 설정을 가져오거나 내보낼 수 있습니다.

이 기능은 카스퍼스키 안티 바이러스가 집과 사무실 컴퓨터에 모두 설치된 경우 등에 유용합니다. 집에서 구성한 방식처럼 사무실에서도 프로그램을 구성할 수 있습니다. 디스크를 사용하여 설정을 파일로 내보낸 후 가져오기 기능을 통해 사무실 컴퓨터에 로드하면 됩니다. 설정은 특별한 구성 파일에 저장됩니다.

- *카스퍼스키 안티 바이러스의 현재 설정을 내보내려면 다음과 같이 하십시오:*

  1. 메인 프로그램 창을 열고 창 상단의 **설정** 링크를 누릅니다.
  2. 열리는 창에서 **옵션** 섹션을 선택합니다.
  3. **프로그램 설정 관리** 섹션에서 **내보내기** 버튼을 누릅니다.

4. 열리는 창에서 구성 파일 이름과 저장 경로를 입력합니다.

- *저장된 구성 파일에서 프로그램 설정을 가져오려면 다음과 같이 하십시오:*

  1. 메인 프로그램 창을 열고 창 상단의 **설정** 링크를 누릅니다.
  2. 열리는 창에서 **옵션** 섹션을 선택합니다.
  3. **프로그램 설정 관리** 섹션에서 **가져오기** 버튼을 누릅니다.
  4. 열리는 창에서 카스퍼스키 안티 바이러스 설정을 가져오려는 파일을 선택합니다.

기본 설정 복원

언제든지 카스퍼스키 안티 바이러스의 기본 설정 또는 권장 설정으로 돌아갈 수 있습니다. 이러한 설정은 가장 적절하다고 간주되며 카스퍼스키 랩에서 권장하는 설정입니다. 프로그램 구성 마법사를 이용해 기본 설정을 복원할 수 있습니다.

열리는 창에 권장 보안 레벨을 복원할 때 저장하거나 저장하지 말아야 할 설정과 구성요소를 결정할 수 있는 메시지가 표시됩니다.

이 목록은 사용자가 변경한 카스퍼스키 안티 바이러스 구성요소의 설정을 포함하고 있습니다. 구성요소에 특별 설정을 지정한 경우 이러한 설정도 목록에 표시됩니다.

이러한 목록은 카스퍼스키 안티 바이러스를 사용하여 개별 작업 및 보안 요구사항을 처리할 경우에 생성됩니다. 목록 생성은 시간이 오래 걸릴 수 있으므로 프로그램의 기본 설정을 복원하기 전에 목록을 저장하는 것이 좋습니다.

구성 마법사를 이용해 복원을 완료하면 복원 시 사용자 지정된 상태를 유지하도록 선택한 설정을 제외하고 모든 구성요소에 **권장** 보안 레벨이 설정됩니다. 또한 마법사를 사용할 때 지정한 설정도 적용됩니다.

- *실시간 감시 설정을 복원하려면 다음과 같이 하십시오:*

  1. 메인 프로그램 창을 열고 창 상단의 **설정** 링크를 누릅니다.
  2. 열리는 창에서 **옵션** 섹션을 선택합니다.
  3. **프로그램 설정 관리** 섹션에서 **초기화** 버튼을 누릅니다.
  4. 열리는 창에서 저장해야 할 설정의 상자에 체크합니다. **다음** 다음 버튼을 누릅니다. 프로그램 구성 마법사가 실행됩니다. 마법사의 지침을 따릅니다.

탐지할 보안위협 및 제외

카스퍼스키 안티 바이러스 설정 창의 **탐지할 보안위협 및 제외** 섹션에서는 다음 처리 방법을 수행할 수 있습니다:

- 탐지 가능한 보안위협 카테고리 선택

- 프로그램에 대한 신뢰 구역 생성

신뢰 구역은 카스퍼스키 안티 바이러스에서 제어하지 않도록 사용자가 생성한 개체 목록입니다. 즉, 카스퍼스키 안티 바이러스 감시 범위에서 제외되는 집합입니다.

신뢰 구역은 신뢰하는 프로그램 목록 및 제외 규칙을 기반으로 생성됩니다.

사용자는 작업하는 개체의 특징 및 컴퓨터에 설치된 프로그램을 기반으로 신뢰 구역을 생성합니다. 예를 들어 카스퍼스키 안티 바이러스가 확실히 안전한 개체 또는 프로그램에 대한 액세스를 차단하는 경우 제외 목록을 생성해야 할 수 있습니다.

참조:

탐지 가능한 보안위협 카테고리 선택 116

신뢰하는 프로그램 선택 116

제외 규칙 117

허락한 파일 제외 마스크 118

허락한 보안위협 형태 마스크 119

탐지 가능한 보안위협 카테고리 선택

카스퍼스키 안티 바이러스는 다양한 종류의 악성 프로그램으로부터 사용자를 보호하며, 선택된 설정과 관계없이 항상 바이러스, 트로이목마 및 해커 유틸리티를 검사하고 치료합니다. 이러한 프로그램은 컴퓨터에 상당한 피해를 입힐 수 있습니다. 컴퓨터의 보안을 강화하도록 탐지되는 보안위협 목록을 확장하여 잠재적으로 위험할 수 있는 여러 프로그램에 대한 제어를 작동해야 합니다.

- *탐지 가능한 보안위협 카테고리를 선택하려면 다음과 같이 하십시오:*

1. 메인 프로그램 창을 열고 창 상단의 **설정** 링크를 누릅니다.
2. 열리는 창에서 **탐지할 보안위협 및 제외** 섹션을 선택합니다. **보안위협 형태** 섹션에서 **설정** 버튼을 누릅니다.
3. 열리는 **탐지할 보안위협** 선택 창에서 컴퓨터를 보호할 보안위협 카테고리를 선택합니다.

신뢰하는 프로그램 선택

신뢰하는 프로그램 목록을 생성하여 해당 파일 및 네트워크 작업을 제어하지 않고 시스템 레지스트리에 액세스하도록 허용할 수 있습니다.

예를 들어 Microsoft Windows 메모장에서 사용하는 개체는 안전하므로 검사할 필요가 없다고 생각할 수 있습니다. 즉, 이 프로그램을 신뢰할 수 있습니다. Microsoft Windows 메모장 프로세스에서 사용하는 개체를 검사에서 제외하려면 메모장 프로그램을 신뢰하는 프로그램 목록에 추가합니다. 이렇게 해도 실행 파일 및 신뢰하는 프로그램의 프로세스에 대해서는 이전과 같이 바이러스 검사가 수행됩니다. 프로그램을 검사에서 완전히 제외하려면 제외 규칙을 사용해야 합니다.

이 밖에도 여러 프로그램에서 정상으로 간주되는 일부 작업이 위험한 것으로 분류될 수 있습니다. 예를 들어 키보드 레이아웃을 자동으로 전환하는 Punto Switcher 와 같은 프로그램은 정기적으로 키보드에 입력되는 텍스트를 가로챕니다. 이러한 프로그램의 특성을 고려하고 해당 작업에 대한 모니터링을 중지하려면 신뢰하는 프로그램 목록에 추가하는 것이 좋습니다.

신뢰하는 프로그램을 검사에서 제외하면 다른 프로그램과의 호환성 문제(예: 카스퍼스키 안티 바이러스와 기타 안티 바이러스 프로그램에서 타사 컴퓨터의 네트워크 트래픽을 이중 검사하는 문제)를 해결할 뿐만 아니라 서버 프로그램 사용 시 중요한 컴퓨터 성능 수준을 향상시킬 수 있습니다.

기본적으로 카스퍼스키 안티 바이러스는 다른 프로그램 프로세스에서 열려 있거나 실행하거나 저장하는 개체를 검사하고 모든 프로그램과 그로 인해 생성되는 네트워크 트래픽을 모니터링합니다.

- *프로그램을 신뢰하는 목록에 추가하려면 다음과 같이 하십시오:*

  1. 메인 프로그램 창을 열고 창 상단의 **설정** 링크를 누릅니다.
  2. 열리는 창에서 **탐지할 보안위협 및 제외** 섹션을 선택합니다.
  3. **제외** 섹션에서 **설정** 버튼을 누릅니다.
  4. 열리는 창에서 **신뢰하는 프로그램** 탭 아래 있는 **추가** 링크를 누릅니다.
  5. 열리는 메뉴에서 프로그램을 선택합니다. **찾아보기** 항목을 선택한 경우 실행 파일 경로를 지정하는 창이 열립니다. 프로그램 항목을 선택한 경우 현재 실행 중인 **프로그램** 목록이 열립니다.
  6. 열리는 **프로그램 제외** 창에서 프로그램에 대한 규칙 설정을 지정합니다.

☑ **네트워크 트래픽 검사 안함** 상자가 체크되어 있는 경우 지정된 프로그램의 트래픽에서 바이러스와 스팸이 검사되지 않지만 방화벽 구성요소에서 수행되는 트래픽 검사에는 영향이 없습니다. 방화벽 설정은 해당 프로그램의 네트워크 활동 분석을 제어합니다.

신뢰하는 프로그램 탭 아래 부분에 있는 편집 또는 삭제 링크를 사용하여 목록에서 신뢰하는 프로그램을 변경 또는 삭제할 수 있습니다. 프로그램을 실제로 삭제하지 않고 목록에서 제거하려면 해당 이름 옆에 있는 상자를 체크해제합니다.

제외 규칙

잠재적으로 위험할 수 있는 소프트웨어는 악성 기능을 갖지 않지만 결함 및 오류가 포함되어 있기 때문에 악성 코드에 대한 보조 구성요소로 사용될 수 있습니다. 이 카테고리에는 원격 관리 프로그램, IRC 클라이언트, FTP 서버, 프로세스를 중지 또는 숨기기 위한 다양한 유틸리티, 키로거, 암호 크래커, 자동 전화 걸기 등이 포함됩니다. 이러한

프로그램은 바이러스로는 분류되지 않습니다(not-a-virus). 애드웨어, 장난 프로그램, 리스크웨어 등과 같은 다양한 형태로 좀더 세분화될 수 있습니다. 카스퍼스키 안티 바이러스에서 탐지되는 잠재적으로 위험할 수 있는 프로그램에 대한 자세한 내용은 진단 명 분류(www.viruslist.com)를 참조하십시오. 이러한 프로그램은 검사 후에 차단될 수 있습니다. 그러나 사용자들이 광범위하게 사용하는 일부 프로그램은 검사에서 제외하도록 선택할 수 있습니다.

예를 들어 Remote Administrator 프로그램을 자주 사용할 수 있습니다. 이것은 원격 접근 프로그램으로서 이 프로그램을 사용하면 원격 컴퓨터에서 작업할 수 있도록 허용됩니다. 카스퍼스키 안티 바이러스는 이 프로그램의 활동을 잠재적으로 위험할 수 있는 것으로 보고 차단할 수 있습니다. 이 프로그램이 차단되지 않기를 원할 경우 프로그램에 대한 제외 규칙을 생성해야 합니다. 이 프로그램은 진단 명 분류에 따라 *not-a-virus:RemoteAdmin.Win32.RAdmin.22* 로 탐지됩니다.

제외 규칙 – 카스퍼스키 안티 바이러스에서 개체를 검사하지 않도록 결정하는 일련의 조건입니다.

진단 명 분류의 보안위협 형태 분류에 따라 특정 형식의 파일을 검사에서 제외하거나 파일 마스크를 사용하거나 특정 영역(예: 폴더 또는 프로그램), 프로그램 프로세스 또는 개체를 제외할 수 있습니다.

보안위협 형태 – 검사 후 카스퍼스키 안티 바이러스에서 개체에 지정되는 상태입니다. 상태는 카스퍼스키 랩의 진단 명 분류에 나열된 악성 프로그램 및 잠재적으로 위험할 수 있는 프로그램 분류를 기준으로 지정됩니다.

제외 항목을 추가하면 규칙이 생성되어 여러 프로그램 구성요소(예: 파일 안티 바이러스, 메일 안티 바이러스, 웹 안티 바이러스)에서 사용되거나 바이러스 검사 작업을 실행할 때 사용될 수 있습니다.

- *제외 규칙을 생성하려면 다음과 같이 하십시오:*

  1. 메인 프로그램 창을 열고 창 상단의 **설정** 링크를 누릅니다.
  2. 열리는 창에서 **탐지할 보안위협 및 제외** 섹션을 선택합니다.
  3. **제외** 섹션에서 **설정** 버튼을 누릅니다.
  4. 열리는 창에서 **제외 규칙** 탭 아래 있는 **추가** 링크를 누릅니다.
  5. 열리는 **제외 규칙** 창에서 제외 규칙 설정을 편집합니다.

참조:

허락된 파일 제외 마스크 118

허락된 보안위협 형태 마스크 119

허락한 파일 제외 마스크

파일 제외 목록을 생성할 때 사용할 수 있는 몇 가지 마스크의 예를 들면 다음과 같습니다:

1. 파일 경로가 없는 마스크:
   - ***.exe** – 확장자가 *exe* 인 모든 파일

- ***.ex?** – 확장자가 *ex?*인 모든 파일. 여기서 **?**는 모든 단일 문자를 나타낼 수 있습니다.
- **test** – 이름이 *test* 인 모든 파일

2. 절대 파일 경로가 있는 마스크:
   - **C:₩dir₩*.*** 또는 **C:₩dir₩*** 또는 **C:₩dir₩** – *C:₩dir₩* 폴더에 있는 모든 파일
   - **C:₩dir₩*.exe** – *C:₩dir₩* 폴더에 있고 확장자가 *exe* 인 모든 파일
   - **C:₩dir₩*.ex?** – *C:₩dir₩* 폴더에 있고 확장자가 *ex?*인 모든 파일. 여기서**?**는 모든 단일 문자를 나타낼 수 있습니다.
   - **C:₩dir₩test** – *C:₩dir₩test* 파일만

     지정한 폴더의 중첩된 모든 폴더에서 파일 검사를 제외하려면 마스크를 생성할 때 ☑ **하위 폴더 포함** 상자를 체크합니다.

3. 파일 경로 마스크:
   - **dir₩*.***, 또는 **dir₩***, 또는 **dir₩** – 모든 *dir₩* 폴더에 있는 모든 파일
   - **dir₩test** – *dir₩* 폴더에 있는 모든 *test* 파일
   - **dir₩*.exe** – 모든 *dir₩* 폴더에 있는 확장자가 *exe* 인 모든 파일
   - **dir₩*.ex?** – 모든 *dir₩* 폴더에 있고 확장자가 *ex?*인 모든 파일. 여기서**?**는 모든 단일 문자를 나타낼 수 있습니다.

     지정한 폴더의 중첩된 모든 폴더에서 파일 검사를 제외하려면 마스크를 생성할 때 ☑ **하위 폴더 포함** 상자를 체크합니다.

진단 명 분류에 따라 보안위협 분류 유형을 지정하는 *.* 및 * 제외 마스크만 사용할 수 있습니다. 이 경우 지정한 보안위협이 개체에서 감지되지 않습니다. 분류 유형을 지정하지 않고 이러한 마스크를 사용하면 감시가 중지됩니다. 제외를 설정하는 경우 subst 명령을 사용하여 파일 시스템 폴더를 기반으로 생성된 네트워크 디스크 또는 네트워크 폴더를 미러링하는 디스크와 관련된 경로는 선택하지 않는 것이 좋습니다. 이렇게 할 경우 서로 다른 사용자가 사용하는 여러 리소스에 동일한 디스크 이름이 지정되어 제외 규칙을 잘못 트리거할 수 있습니다.

허락한 보안위협 형태 마스크

진단 명 분류에 따라 특정 보안위협을 제외하도록 마스크를 추가하는 경우 다음 설정을 지정할 수 있습니다:

- *www.viruslist.com* 의 진단 명 분류에 지정된 보안위협 이름(예: *not-a-virus:RiskWare.RemoteAdmin.RA.311* 또는 *Flooder.Win32.Fuxx*)
- 마스크를 사용한 보안위협 이름. 예:

- **not-a-virus*** – 합법적이지만 잠재적으로 위험할 수 있는 프로그램 및 장난 프로그램을 검사에서 제외합니다.
- ***Riskware.*** – 리스크웨어를 검사에서 제외합니다.
- ***RemoteAdmin.*** – 모든 원격 관리 프로그램을 검사에서 제외합니다.

네트워크

프로그램 설정 창의 **네트워크** 섹션에서는 카스퍼스키 안티 바이러스에서 감시되는 포트를 선택하고 암호화된 연결 검사를 구성할 수 있습니다:

- 감시하는 포트 목록 생성
- 암호화된 연결 검사 모드(SSL 프로토콜 사용) 작동/중지
- 프록시 서버 설정 편집

참조:

감시하는 포트 목록 생성 120

암호화된 연결 검사 121

Mozilla Firefox 에서 암호화된 연결 검사 122

Opera 에서 암호화된 연결 검사 123

프록시 서버 설정 124

감시하는 포트 목록 생성

메일 안티 바이러스, 웹 안티 바이러스 및 안티 스팸과 같은 실시간 감시 구성요소는 특정 프로토콜을 통해 전송되는 데이터 스트림을 감시하고 컴퓨터에서 열려진 특정 포트를 전달합니다. 예를 들어 메일 안티 바이러스는 SMTP 프로토콜을 통해 전송된 정보를 분석하고 웹 안티 바이러스는 HTTP 패킷을 분석합니다.

두 가지 포트 감시 모드 중 하나를 선택할 수 있습니다:

- **모든 네트워크 포트 감시**
- **선택한 포트만 감시.** 전송된 이메일 및 HTTP 트래픽에 사용되는 포트 목록이 프로그램 패키지에 포함됩니다.

- *감시하는 포트 목록에 포트를 추가하려면:*

  1. 메인 프로그램 창을 열고 창 상단의 **설정** 링크를 누릅니다.
  2. 열리는 창에서 **네트워크** 섹션을 선택합니다.
  3. **감시하는 포트** 섹션에서 **선택** 버튼을 누릅니다.
  4. 열리는 **네트워크 포트** 창에서 **추가** 링크를 누릅니다.
  5. 열리는 **네트워크 포트** 창에서 필요한 데이터를 지정합니다.

- *감시하는 포트 목록에서 포트를 제외하려면:*

  1. 메인 프로그램 창을 열고 창 상단의 **설정** 링크를 누릅니다.
  2. 열리는 창에서 **네트워크** 섹션을 선택합니다.
  3. **감시하는 포트** 섹션에서 **선택** 버튼을 누릅니다.
  4. 열리는 **네트워크 포트** 창에서 포트 설명 옆에 있는 ☑ 상자를 체크해제합니다.

- *모든 포트를 감시할 프로그램 목록을 생성하려면 다음과 같이 하십시오:*

  1. 메인 프로그램 창을 열고 창 상단의 **설정** 링크를 누릅니다.
  2. 열리는 창에서 **네트워크** 섹션을 선택합니다.
  3. **감시하는 포트** 섹션에서 **선택** 버튼을 누릅니다.
  4. 열리는 **네트워크 포트** 창에서 ☑ **지정한 프로그램의 모든 포트 감시** 상자를 체크하고 아래 섹션에서 **추가** 링크를 누릅니다.
  5. 열리는 메뉴에서 프로그램을 선택합니다. **찾아보기** 항목을 선택한 경우 실행 파일 경로를 지정하는 창이 열립니다. **프로그램** 항목을 선택한 경우 현재 실행 중인 프로그램 목록이 열립니다.
  6. 열리는 **프로그램** 창에서 선택한 프로그램에 대한 설명을 지정합니다.

암호화된 연결 검사

SSL(Secure Sockets Layer) 프로토콜을 사용하여 연결하면 인터넷상의 데이터 교환 채널이 보호됩니다. SSL 프로토콜을 통해 전자 인증서를 사용하여 데이터를 교환하는 당사자를 식별하고 전송되는 데이터를 인코딩하며 전송 과정의 무결성을 보장할 수 있습니다.

그러나 이러한 프로토콜 기능은 해커가 악성 프로그램을 유포하는 데 이용될 수 있습니다. 대부분의 안티 바이러스 프로그램에서 SSL 트래픽을 검사하지 않기 때문입니다.

카스퍼스키 안티 바이러스는 카스퍼스키 랩의 인증서를 사용하여 암호화된 연결을 검사합니다. 이 인증서는 연결이 안전하지 여부를 확인하도록 항상 사용됩니다.

SSL 프로토콜을 통한 추가 트래픽 검사는 설치된 카스퍼스키 랩 인증서를 사용하여 수행됩니다. 서버에 연결할 때 잘못된 인증서가 탐지되는 경우(예: 인증서를 침입자가 교체한 경우) 인증서를 적용 또는 취소하거나 인증서에 대한 정보를 확인하라는 팝업 알림 메시지가 나타납니다. 카스퍼스키 안티 바이러스가 자동 모드로 작동하는 경우 잘못된 인증서를 사용한 연결이 알림 없이 종료됩니다.

- *암호화된 연결 검사를 작동하려면 다음과 같이 하십시오:*

  1. 메인 프로그램 창을 열고 창 상단의 **설정** 링크를 누릅니다.
  2. 열리는 창에서 **네트워크** 섹션을 선택합니다.
  3. 열리는 창에서 **암호화된 연결(SSL) 검사** 상자를 선택하고 **인증서 설치** 버튼을 누릅니다.
  4. 열리는 창에서 **인증서 설치** 버튼을 누릅니다. 그러면 마법사가 시작되어 안내를 따라 인증서를 설치하면 됩니다.

인증서 자동 설치는 Microsoft Internet Explorer에서만 가능합니다. Mozilla Firefox 또는 Opera에서 암호화된 연결을 검사하려면 카스퍼스키 랩의 인증서를 수동으로 설치해야 합니다.

MOZILLA FIREFOX 에서 암호화된 연결 검사

Mozilla Firefox 브라우저에서는 Microsoft Windows 인증서 저장소를 사용하지 않습니다. Firefox 를 사용하여 SSL 연결을 검사하려면 카스퍼스키 랩의 인증서를 수동으로 설치해야 합니다.

- *카스퍼스키 랩의 인증서를 설치하려면 다음과 같이 하십시오:*

  1. 브라우저 메뉴에서 **Tools** (도구) → **Settings** (설정) 항목을 선택합니다.
  2. 열리는 창에서 **Additional**(고급) 섹션을 선택합니다.
  3. **Certificates**(인증서) 섹션에서 **Security**(보안) 탭을 선택하고 **Viewing certificates**(인증서 보기) 버튼을 누릅니다.
  4. 열리는 창에서 **Certification Centers**(인증 센터) 탭을 선택하고 **Restore**(복원) 버튼을 누릅니다.
  5. 열리는 창에서 카스퍼스키 랩 인증서 파일을 선택합니다. 카스퍼스키 랩 인증서 파일 경로는 다음과 같습니다. *%AllUsersProfile%₩Application?Data₩Kaspersky?Lab₩AVP8₩Data₩Cert₩(fake)Kaspersky?Anti-Virus?personal?root?certificate.cer.*
  6. 열리는 창에서 설치된 인증서로 검사할 작업에 해당하는 상자를 체크합니다. 인증서에 대한 정보를 보려면 **View**(보기) 버튼을 누릅니다.

- *Mozilla Firefox 버전 3.x 에 대해 카스퍼스키 랩의 인증서를 설치하려면 다음과 같이 하십시오:*

  1. 브라우저 메뉴에서 **Tools**(도구) → **Settings**(설정) 항목을 선택합니다.
  2. 열리는 창에서 **Additional**(고급) 섹션을 선택합니다.
  3. **Encryption**(암호화) 탭에서 **Viewing certificates**(인증서 보기) 버튼을 누릅니다.
  4. 열리는 창에서 **Certification Centers**(인증 센터) 탭을 선택하고 **Import**(가져오기) 버튼을 누릅니다.
  5. 열리는 창에서 카스퍼스키 랩 인증서 파일을 선택합니다. 카스퍼스키 랩 인증서 파일 경로는 다음과 같습니다. *%AllUsersProfile%₩Application?Data₩Kaspersky?Lab₩AVP8₩Data₩Cert₩(fake)Kaspersky?Anti-Virus?personal?root?certificate.cer*
  6. 열리는 창에서 설치된 인증서로 검사할 작업에 해당하는 상자를 체크합니다. 인증서에 대한 정보를 보려면 **View**(보기) 버튼을 누릅니다.

Microsoft Windows Vista를 실행하는 컴퓨터의 경우 카스퍼스키 랩 인증서 파일 경로는 다음과 같습니다. *%AllUsersProfile%₩Kaspersky?Lab₩AVP8₩Data₩Cert₩(fake)Kaspersky?Anti-Virus?personal?root?certificate.cer*.

OPERA 에서 암호화된 연결 검사

Opera 브라우저에서는 Microsoft Windows 인증서 저장소를 사용하지 않습니다. Opera 를 사용하여 SSL 연결을 검사하려면 카스퍼스키 랩의 인증서를 수동으로 설치해야 합니다.

- *카스퍼스키 랩의 인증서를 설치하려면 다음과 같이 하십시오:*

  1. 브라우저 메뉴에서 **Tools**(도구) → **Settings**(설정) 항목을 선택합니다.
  2. 열리는 창에서 **Additional**(고급) 섹션을 선택합니다.
  3. 창 왼쪽에서 **Security**(보안) 탭을 선택하고 **Manage Certificates**(인증서 관리) 버튼을 누릅니다.
  4. 열리는 창에서 **Vendors**(공급사) 탭을 선택하고 **Import**(가져오기) 버튼을 누릅니다.
  5. 열리는 창에서 카스퍼스키 랩 인증서 파일을 선택합니다. 카스퍼스키 랩 인증서 파일 경로는 다음과 같습니다. *%AllUsersProfile%₩Application?Data₩Kaspersky?Lab₩AVP8₩Data₩Cert₩(fake)Kaspersky?Anti-Virus?personal?root?certificate.cer*
  6. 열리는 창에서 **Install**(설치) 버튼을 누릅니다. 카스퍼스키 랩 인증서가 설치됩니다. 인증서에 대한 정보를 보고 인증서가 사용되는 처리 방법을 선택하려면 목록에서 인증서를 선택한 후 **View**(보기) 버튼을 누릅니다.

- *버전 9.x 에 대해 카스퍼스키 랩의 인증서를 설치하려면 다음과 같이 하십시오:*

  1. 브라우저 메뉴에서 **Tools**(도구) → **Settings**(설정) 항목을 선택합니다.

2. 열리는 창에서 **Additional**(고급) 섹션을 선택합니다.
3. 창 왼쪽에서 **Security**(보안) 탭을 선택하고 **Manage Certificates**(인증서 관리) 버튼을 누릅니다.
4. 열리는 창에서 **Certification Centers**(인증 센터) 탭을 선택하고 **Import**(가져오기) 버튼을 누릅니다.
5. 열리는 창에서 카스퍼스키 랩 인증서 파일을 선택합니다. 카스퍼스키 랩 인증서 파일 경로는 다음과 같습니다. *%AllUsersProfile%₩Application?Data₩Kaspersky?Lab₩AVP8₩Data₩Cert₩(fake)Kaspersky?Anti-Virus?personal?root?certificate.cer*
6. 열리는 창에서 **Install**(설치) 버튼을 누릅니다. 카스퍼스키 랩 인증서가 설치됩니다.

Microsoft Windows Vista를 실행하는 컴퓨터의 경우 카스퍼스키 랩 인증서 파일 경로는 다음과 같습니다. *%AllUsersProfile%₩Kaspersky?Lab₩AVP8₩Data₩Cert₩(fake)Kaspersky?Anti-Virus?personal?root?certificate.cer*

프록시 서버 설정

프록시 서버를 통해 컴퓨터에 인터넷을 연결한 경우 연결 설정을 편집해야 할 수 있습니다. 카스퍼스키 안티 바이러스는 이러한 설정을 특정 실시간 감시 구성요소에 사용하며, 데이터베이스 및 프로그램 모듈 업데이트에도 사용합니다.

네트워크에 비 표준 포트를 사용한 프록시 서버가 포함된 경우 포트 번호를 감시하는 포트 목록에 추가해야 합니다.

- *프록시 서버를 구성하려면 다음과 같이 하십시오:*

1. 메인 프로그램 창을 열고 창 상단의 **설정** 링크를 누릅니다.
2. 열리는 창에서 **네트워크** 섹션을 선택합니다.
3. **프록시 서버** 섹션에서 **프록시 서버 설정** 버튼을 누릅니다.
4. 열리는 **프록시 서버 설정** 창에서 프록시 서버 설정을 변경합니다.

알림

카스퍼스키 안티 바이러스 작업 중에는 다양한 이벤트가 발생할 수 있습니다. 정보를 전달하는 이벤트일 수도 있고 중요한 정보가 포함된 이벤트일 수 있습니다. 예를 들어 프로그램 업데이트를 성공적으로 완료했다는 것을 알리거나 즉시 제거해야 하는 특정 구성요소 작업에서 오류가 발생했음을 알리는 이벤트일 수 있습니다.

카스퍼스키 안티 바이러스 작업의 이벤트를 확인하려면 알림 서비스를 사용하십시오.

기본적으로 사용자는 이벤트에 대해 소리 알림과 함께 팝업 메시지로 알림을 받습니다.

알림은 다음 방법 중 하나로 전달될 수 있습니다:

- 시스템 트레이에서 카스퍼스키 안티 바이러스 아이콘 위에 나타나는 팝업 메시지
- 소리 알림
- 이메일 메시지

- *알림 전달을 중지하려면 다음과 같이 하십시오:*

1. 메인 프로그램 창을 열고 창 상단의 **설정** 링크를 누릅니다.
2. 열리는 창에서 **알림** 섹션을 선택합니다.
3. ☑ **이벤트 알림 작동** 상자를 체크해제합니다.

알림 전달을 중지한 경우에도 카스퍼스키 안티 바이러스 작업에서 발생하는 이벤트에 대한 정보는 작업 보고서에 기록됩니다.

- *알림 전달 방법을 선택하려면 다음과 같이 하십시오:*

1. 메인 프로그램 창을 열고 창 상단의 **설정** 링크를 누릅니다.
2. 열리는 창에서 **알림** 섹션을 선택하고 **설정** 버튼을 누릅니다.
3. 열리는 **알림** 창에서 알림 전달 방법을 선택합니다.

참조:

소리 알림 중지 125

이메일로 알림 전달 126

소리 알림 중지

기본적으로 모든 알림에는 소리 알림이 포함되며 Microsoft Windows 소리 구성표가 사용됩니다. ☑ **Windows 기본 소리 사용** 상자를 통해 사용되는 구성표를 변경할 수 있습니다. 상자를 체크해제하면 이전 프로그램 버전의 소리 구성표가 사용됩니다.

- *소리 알림을 중지하려면 다음과 같이 하십시오:*

1. 메인 프로그램 창을 열고 창 상단의 **설정** 링크를 누릅니다.
2. 열리는 창에서 **알림** 섹션을 선택합니다.
3. ☑ **소리 알림 작동** 상자를 체크해제합니다.

이메일로 알림 전달

이메일로 알림을 전달하려면 전달 설정을 편집합니다.

- *이메일 알림 전달 설정을 수정하려면 다음과 같이 하십시오:*

  1. 메인 프로그램 창을 열고 창 상단의 **설정** 링크를 누릅니다.
  2. 열리는 창에서 **알림** 섹션을 선택합니다.
  3. ☑ **이메일 알림 작동** 상자를 체크하고 **이메일 설정** 버튼을 누릅니다.
  4. 열리는 **이메일 알림 설정** 창에서 전달 설정을 지정합니다.

리포트 및 저장소

이 섹션에는 카스퍼스키 안티 바이러스 데이터 파일을 사용한 작업을 제어하는 설정이 포함되어 있습니다.

*프로그램 데이터 파일*은 카스퍼스키 안티 바이러스에서 격리되었거나 백업으로 이동한 개체 및 프로그램 구성요소 작업에 대한 리포트가 포함된 파일입니다.

이 섹션에서는 다음을 수행할 수 있습니다:

- 리포트 생성 및 저장
- 격리 및 백업 설정 구성

참조:

리포트에 이벤트 기록 127
프로그램 리포트 삭제 127
리포트 저장 127
감염 위험 개체에 대한 격리저장소 128
위험 개체의 복사본 백업 128
격리된 개체에 대한 처리 방법 129
격리 저장소 및 백업 개체 저장 129
리포트 140

리포트에 이벤트 기록

중요하지 않은 이벤트, 레지스트리 및 파일 시스템 이벤트에 대한 정보를 리포트에 추가할 수 있습니다. 기본적으로 이러한 이벤트는 리포트에 기록되지 않습니다.

- *중요하지 않은 이벤트, 레지스트리 및 파일 시스템 이벤트에 대한 정보를 리포트에 추가하려면 다음과 같이 하십시오:*

  1. 메인 프로그램 창을 열고 창 상단의 **설정** 링크를 누릅니다.
  2. 열리는 창에서 **리포트 및 저장소** 섹션을 선택합니다.
  3. **리포트** 섹션에서 필요한 상자를 체크합니다.

프로그램 리포트 삭제

카스퍼스키 안티 바이러스 작업에 대한 정보는 리포트에 기록됩니다. 이러한 리포트를 삭제할 수 있습니다.

- *프로그램 리포트를 삭제하려면 다음과 같이 하십시오*:

  1. 메인 프로그램 창을 열고 창 상단의 **설정** 링크를 누릅니다.
  2. 열리는 창에서 **리포트 및 저장소** 섹션을 선택합니다.
  3. **리포트** 섹션에서 **지우기** 버튼을 누릅니다.
  4. 열리는 **리포트 파일 삭제** 창에서 삭제하려는 리포트 카테고리의 상자를 체크합니다.

리포트 저장

이벤트 리포트의 최대 저장 기간을 지정할 수 있습니다(**리포트 저장 기간** 상자). 기본값은 30 일입니다. 이 기간이 끝나면 개체가 삭제됩니다. 최대 저장 기간을 변경할 수 있으며, 리포트에 설정된 모든 제한을 취소할 수도 있습니다. 이 밖에도 리포트 파일의 최대 크기를 지정할 수 있습니다(**최대 파일 크기** 상자). 최대 크기 기본값은 1024MB 입니다. 최대 크기에 도달하면 파일 컨텐츠를 새 레코드로 덮어씁니다. 리포트 크기에 설정된 제한을 취소하거나 다른 값을 입력할 수 있습니다.

- *리포트 저장 설정을 구성하려면 다음과 같이 하십시오:*

  1. 메인 프로그램 창을 열고 창 상단의 **설정** 링크를 누릅니다.
  2. 열리는 창에서 **리포트 및 저장소** 섹션을 선택합니다.
  3. 열리는 창의 **리포트** 섹션에서 필요한 상자를 체크하고 최대 리포트 크기 및 저장 기간을 변경합니다(필요한 경우).

감염 위험 개체에 대한 격리 저장소

*격리 저장소*는 바이러스 감염 위험이 있는 개체를 저장하는 특별한 저장소입니다.

*감염 위험이 있는 개체*는 바이러스 또는 바이러스의 변형으로 인한 감염이 의심되는 개체입니다.

감염 위험이 있는 개체는 파일 안티 바이러스, 메일 안티 바이러스, 사전 방역에서 또는 바이러스 검사 과정 중에 탐지 및 격리될 수 있습니다.

파일 안티 바이러스 및 메일 안티 바이러스 작업 결과로 또는 바이러스 검사 중에 개체가 격리 저장소에 배치되는 경우는 다음과 같습니다:

- *분석되는 개체의 코드가 알려진 보안위협과 유사하지만 부분적으로 변형된 경우.*

  카스퍼스키 안티 바이러스 데이터베이스에는 현재까지 카스퍼스키 랩 전문가들에 의해 조사된 보안위협에 대한 정보가 포함되어 있습니다. 악성 프로그램이 변형되어 아직 데이터베이스에 입력되지 않은 경우 카스퍼스키 안티 바이러스에서는 변형된 악성 프로그램에 감염된 개체를 감염 위험이 있는 개체로 분류하여 해당 감염과 유사한 보안위협을 알려줍니다.

- *탐지되는 개체의 코드가 악성 프로그램의 구조를 상기시키지만 데이터베이스에 유사한 것이 기록되지 않은 경우.*

  신종 보안위협일 가능성이 상당히 높으므로 카스퍼스키 안티 바이러스는 해당 개체를 감염 위험 개체로 분류합니다.

파일은 *휴리스틱 코드 분석기*를 통해 바이러스 감염 위험이 있는 것으로 식별됩니다. 이 메커니즘은 상당히 효과적이며 정상적인 개체를 탐지하는 일은 거의 없습니다.

사전 방역 구성요소는 행동 분석 결과 개체의 일련의 활동이 의심을 불러일으키는 경우 개체를 격리 저장소에 배치합니다.

개체를 격리 저장소에 배치하는 경우 개체가 복사되는 것이 아니라 이동됩니다. 즉, 개체가 디스크 또는 이메일에서 삭제되고 격리 저장소 폴더에 저장됩니다. 격리 저장소의 파일은 특별한 형식으로 저장되며 위험하지 않습니다.

데이터베이스 업데이트 후 카스퍼스키 안티 바이러스는 보안위협을 분명하게 식별하여 처리할 가능성이 있습니다. 이 때문에 카스퍼스키 안티 바이러스는 매번 업데이트 후에 격리 저장소 개체를 검사합니다.

위험 개체의 복사본 백업

치료 중에는 개체의 무결성을 유지할 수 없는 경우가 있습니다. 치료된 파일에 중요한 정보가 포함되어 있던 경우 치료 후 일부 또는 전체에 접근하지 못할 수 있습니다. 그럴 경우 백업 복사본에서 원래 개체를 복원해야 합니다.

*백업 복사본*은 위험한 원래 개체의 복사본으로서 처음 치료 또는 삭제할 때 생성되어 백업 저장소에 저장됩니다.

*백업 저장소*는 처리 또는 삭제 후 위험한 개체의 백업 복사본이 포함되는 특별한 저장소입니다. 백업 저장소의 주요 기능은 원래 개체를 언제든지 복원하는 것입니다. 백업 저장소의 파일은 특별한 형식으로 저장되며 위험하지 않습니다.

격리된 개체에 대한 처리 방법

격리된 개체에 대해 다음 처리 방법을 수행할 수 있습니다:

- 감염이 의심되는 파일을 격리합니다.
- 최신 카스퍼스키 안티 바이러스 데이터베이스를 사용하여 격리 저장소에서 감염 위험이 있는 모든 개체를 검사하고 치료합니다.
- 격리 저장소로 이동하기 전의 원래 폴더 또는 사용자가 선택한 폴더로 파일을 복원합니다.
- 격리된 개체 또는 선택한 개체 그룹을 삭제합니다.
- 격리된 개체를 카스퍼스키 랩에 전송하여 분석을 받습니다.

- *격리된 개체에 대한 처리 방법을 수행하려면 다음과 같이 하십시오:*

1. 메인 프로그램 창을 열고 **격리 저장소** 링크를 누릅니다.
2. 열리는 창의 **탐지된 보안위협** 탭에서 필요한 작업을 수행합니다.

격리 저장소 및 백업 개체 저장

격리 및 백업 저장소에 대한 다음 설정을 편집할 수 있습니다:

- 격리된 개체 및 백업 복사본 개체의 최대 저장 기간을 지정할 수 있습니다(☑ **개체 저장 기간** 상자). 개체 저장 기간 기본값은 30 일입니다. 이 기간이 끝나면 개체가 삭제됩니다. 최대 저장 기간을 변경하거나 이 제한을 모두 제거할 수 있습니다.
- 데이터 저장 영역의 최대 크기를 지정할 수 있습니다(☑ **최대 크기** 상자). 최대 크기 기본값은 100MB 입니다. 리포트 크기 제한을 취소하거나 다른 값을 설정할 수 있습니다.

- *격리 및 백업 저장소 설정을 구성하려면 다음과 같이 하십시오:*

1. 메인 프로그램 창을 열고 창 상단의 **설정** 링크를 누릅니다.
2. 열리는 창에서 **리포트 및 저장소** 섹션을 선택합니다.
3. **격리 및 백업 저장소** 섹션에서 필요한 상자를 체크하고 데이터 저장 영역의 최대 크기를 입력합니다(필요한 경우).

정보 제공

전 세계적으로 날마다 수많은 신종 보안위협이 나타나고 있습니다. 카스퍼스키 랩은 신종 보안위협 형태 및 경로에 대한 통계를 간편하게 수집하고 제거 방법을 신속히 마련할 수 있도록 *카스퍼스키 시큐리티 네트워크* 서비스를 사용할 것을 권장합니다.

카스퍼스키 시큐리티 네트워크를 사용하면 특정 정보를 카스퍼스키 랩에 보내도록 제안됩니다. 다음과 같은 데이터가 전송됩니다:

- 카스퍼스키 랩 프로그램에서 사용자 컴퓨터에 할당한 고유 확인자. 이 확인자는 사용자 컴퓨터의 하드웨어 설정을 파악하며 개인 정보는 포함되어 있지 않습니다.
- 프로그램 구성요소에서 탐지한 보안위협에 대한 정보. 정보 구조 및 컨텐츠는 탐지되는 보안위협 형태에 따라 다릅니다.
- 운영 체제에 대한 정보: 운영 체제 버전, 설치된 서비스 팩, 다운로드되는 서비스 및 드라이버, 브라우저 및 메일 클라이언트 버전, 브라우저 확장자, 설치된 카스퍼스키 랩 프로그램의 버전 번호

- *카스퍼스키 시큐리티 네트워크에서 통계 보내기를 작동하려면 다음과 같이 하십시오:*

1. 메인 프로그램 창을 열고 창 상단의 **설정** 링크를 누릅니다.
2. 열리는 창에서 **정보 제공** 섹션을 선택합니다.
3. **[동의] 카스퍼스키 시큐리티 네트워크에 참가하겠습니다** 상자를 체크합니다.

프로그램 인터페이스

다양한 그래픽 및 색상 구성표를 만들고 사용하여 카스퍼스키 안티 바이러스 인터페이스를 변경할 수 있습니다. 또한 다양한 활성 인터페이스 요소(예: Microsoft Windows 작업 표시줄 알림 영역의 프로그램 아이콘, 팝업 메시지)를 사용하도록 구성할 수 있습니다.

참조:

활성 인터페이스 요소 130

프로그램 스킨 131

활성 인터페이스 요소

활성 인터페이스 요소(예: 시스템 트레이의 카스퍼스키 안티 바이러스 아이콘 및 팝업 메시지)에 대한 설정을 구성하려면 카스퍼스키 안티 바이러스의 다음 기능을 사용하십시오:

작업 표시줄 아이콘 애니메이션 작동

프로그램에서 수행하는 작업에 따라 시스템 트레이의 프로그램 아이콘이 바뀝니다. 예를 들어 스크립트를 검사하는 경우 아이콘 백그라운드에 스크립트에 대한 짧은 설명이 나타납니다. 이메일 메시지를 검사하는 경우 문자 그림이 나타납니다. 카스퍼스키 인터넷 아이콘 애니메이션이 작동됩니다. 이 경우 컴퓨터의 감시 상태가 반영됩니다. 감시가 작동되는 경우 아이콘이 컬러로 나타나고 중지 또는 일시 중지된 경우 회색으로 나타납니다.

반투명 창 기능 작동

사용자의 즉각적인 주의 또는 의사 결정이 필요한 모든 프로그램 작업은 시스템 트레이 프로그램 아이콘 위에 팝업 메시지로 표시됩니다. 메시지 창은 사용자의 작업을 방해하지 않도록 반투명하며, 마우스 커서로 가리키면 메시지 창의 반투명성이 사라집니다.

뉴스 알림 작동

기본적으로 뉴스가 수신되면 시스템 트레이에 특수한 아이콘이 표시되며, 아이콘을 누르면 뉴스가 포함된 창이 표시됩니다.

Microsoft Windows 로그인 창 위에 "Protected by Kaspersky Lab" 보이기

카스퍼스키 안티 바이러스가 시작되면 기본적으로 화면 오른쪽 상단에 이 표시기가 나타나서 컴퓨터가 모든 형태의 보안위협으로부터 보호되고 있음을 알립니다.

Microsoft Windows Vista를 실행하는 컴퓨터에 설치된 경우 이 옵션을 사용할 수 없습니다.

- *활성 인터페이스 요소를 구성하려면 다음과 같이 하십시오:*

1. 메인 프로그램 창을 열고 창 상단의 **설정** 링크를 누릅니다.
2. 열리는 창에서 **인터페이스** 섹션을 선택합니다.
3. **작업 표시줄 알림 영역 블록의 아이콘**에서 필요한 상자를 체크 또는 체크해제합니다.

프로그램 스킨

카스퍼스키 안티 바이러스 인터페이스에서 사용하는 모든 색상, 글씨, 아이콘 및 텍스트를 수정할 수 있습니다. 자신만의 프로그램 스킨을 만들거나 다른 언어로 지역화할 수 있습니다.

- *다른 프로그램 스킨을 사용하려면 다음과 같이 하십시오:*

1. 메인 프로그램 창을 열고 창 상단의 **설정** 링크를 누릅니다.
2. 열리는 창에서 **인터페이스** 섹션을 선택합니다.
3. **스킨** 섹션의 **다른 스킨 사용** 상자를 체크하여 스킨을 활성화합니다. 입력 칸에 스킨 설정이 포함된 폴더를 지정합니다. 폴더를 선택하려면 **찾아보기** 버튼을 누릅니다.

카스퍼스키 안티 바이러스 프로필 사용

전체 화면 모드에서 게임 프로그램과 같은 일부 프로그램을 사용할 경우 카스퍼스키 안티 바이러스의 특정 기능(예: 알림 서비스)을 중지해야 할 수도 있습니다. 또한 이러한 프로그램을 실행하려면 상당량의 시스템 리소스가 필요하므로 특정한 카스퍼스키 안티 바이러스 작업을 실행할 경우 성능이 저하될 수 있습니다.

전체 화면 모드로 프로그램을 실행할 때마다 수동으로 알림을 중지하고 작업을 일시 중지하는 것을 피하기 위해 카스퍼스키 안티 바이러스는 게임 프로필을 사용하여 설정을 일시적으로 편집할 수 있는 옵션을 제공합니다. 게임 프로파일을 사용하면 전체 화면 모드로 전환할 때 모든 구성요소의 설정을 편집하는 동시에 모드 종료 시 변경 사항을 롤백할 수 있습니다.

전체 화면 모드로 전환하면 이벤트 알림이 자동으로 중지됩니다. 또한 다음 설정을 지정할 수 있습니다:

- **자동으로 처리 방법 선택**. 이 설정을 선택하면 자동으로 선택된 처리가 대응 방법으로 모든 구성요소에 적용되고 설정에서 **사용자 확인 후 처리** 옵션이 선택됩니다. 따라서 프로그램이 자동으로 처리를 선택하므로 탐지된 위협에 대한 처리를 선택하라는 메시지가 표시되지 않습니다.
- **업데이트 실행 안함** 및 **스케줄된 검사 작업 실행 안함**. 전체 화면 프로그램의 성능 저하를 방지하기 위해서는 이러한 설정을 사용하는 것이 좋습니다.

- *게임 프로필을 작동하려면 다음과 같이 하십시오:*

1. 메인 프로그램 창을 열고 창 상단의 **설정** 링크를 누릅니다.
2. 열리는 창에서 **게임 전용 프로필** 섹션을 선택합니다.
3. **게임 전용 프로필 작동** 상자를 체크하고 원하는 설정을 지정합니다.

추가 기능

컴퓨터의 보안은 운영 체제의 기능과 취약점을 이용하는 방법에 대한 전문 지식이 필요한 어려운 작업입니다. 또한 시스템 보안에 대한 정보가 매우 많고 다양하므로 분석하고 처리하기가 어렵습니다.

컴퓨터 보안을 제공하는 데 있어서 특정 작업을 손쉽게 해결할 수 있도록 카스퍼스키 안티 바이러스 패키지에는 마법사 및 도구 세트가 포함됩니다.

- 보안 키보드 - 키보드에 입력한 데이터를 가로채지 못하도록 합니다.
- 응급 복구 디스크 제작 마법사 - 바이러스 공격을 받거나 운영 체제의 시스템 파일이 손상되어 재부팅할 수 없는 경우 시스템의 운용성을 복원합니다.
- 브라우저 보안 마법사 - 보안 관점에서 가장 먼저 Microsoft Internet Explorer 브라우저 설정을 분석하고 평가합니다.
- 시스템 복구 마법사 - 시스템에서 악성 프로그램 개체의 흔적을 제거합니다.
- 개인정보보호 마법사 - 시스템에서 사용 활동 흔적을 검색하여 제거합니다.

참조:

보안 키보드 133

응급 복구 디스크 134

브라우저 구성 137

감염 후 복원 138

개인정보보호 마법사 138

보안 키보드

컴퓨터 작업 중에는 개인 정보 또는 사용자 이름과 암호를 입력해야 하는 상황이 자주 발생합니다. 예를 들어 온라인 스토어와 같은 인터넷 사이트에 등록할 수 있습니다.

이러한 개인 정보가 키 입력을 등록하는 프로그램인 하드웨어 키보드 인터셉터 또는 키로거를 사용하여 가로채일 위험이 있습니다.

보안 키보드 도구는 키보드에 입력되는 데이터가 가로채이지 않도록 방지합니다.

개인 정보 입력을 요구하는 웹사이트가 해킹당한 경우 침입자가 정보를 직접 가져가므로 보안 키보드를 통해 개인 정보를 보호할 수 없습니다.

스파이웨어로 분류되는 많은 프로그램은 스크린샷을 만드는 함수를 가지고 있습니다. 만들어진 스크린샷은 침입자에게 전송되어 추가 분석을 거쳐 개인 정보를 훔치는 데 사용됩니다. 보안 키보드는 입력되는 개인 정보를 스크린샷을 사용하여 가로채지 못하도록 방지합니다.

보안 키보드는 Microsoft Internet Explorer 및 Mozilla Firefox로 작업하는 경우에만 개인 정보 가로채기를 방지할 수 있습니다.

보안 키보드를 사용하려면 다음과 같이 하십시오:

1. 메인 프로그램 창을 엽니다.
2. 창 왼쪽에서 **보안 서비스+** 섹션을 선택하고 **보안 키보드** 버튼을 누릅니다.
3. 보안 키보드의 버튼을 눌러 필요한 데이터를 입력합니다. 데이터를 올바른 칸에 입력해야 합니다. 보안 키보드에서 기능 키(**Shift**, **Alt**, **Ctrl**)를 누르면 특정 모드가 수정됩니다. 예를 들어 **Shift** 키를 누르면 모든 문자가 대문자로 입력됩니다. 특수 모드를 종료하려면 같은 기능 키를 다시 한 번 누릅니다.

응급 복구 디스크

카스퍼스키 안티 바이러스에는 응급 복구 디스크를 생성할 수 있는 서비스가 포함되어 있습니다.

응급 복구 디스크는 감염된 x86 호환 컴퓨터를 검사 및 치료할 수 있도록 설계되었으며, 컴퓨터의 감염 수준이 운영 체제에서 실행되는 안티 바이러스 프로그램 또는 악성 프로그램 삭제 유틸리티(카스퍼스키 AVP 도구 등)를 사용하여 치료할 수 없는 경우에 사용해야 합니다. 이 경우 운영 체제가 로드될 때 악성 프로그램이 제어할 수 없으므로 치료 효율이 더 높습니다.

응급 복구 디스크는 다음을 포함한 Linux 코어 기반의 .iso 파일입니다:

- 시스템 및 구성 Linux 파일
- 운영 체제 진단 유틸리티 세트
- 추가 도구 세트(파일 매니저 등)
- 카스퍼스키 응급 복구 디스크 파일
- 안티 바이러스 데이터베이스를 포함하는 파일

운영 체제가 손상된 컴퓨터는 CD/DVD-ROM 장치에서 부팅됩니다. 이렇게 하려면 컴퓨터에 해당 장치가 있어야 합니다.

- *응급 복구 디스크를 제작하려면 다음과 같이 하십시오:*

  1. 메인 프로그램 창을 엽니다.
  2. 창 왼쪽에서 **보안 서비스+** 섹션을 선택합니다.
  3. **응급 복구 디스크 제작** 버튼을 눌러 디스크 제작 마법사를 실행합니다.
  4. 마법사의 지침을 따르십시오.
  5. 마법사가 제공하는 파일을 사용하여 부트 CD/DVD 를 생성합니다. 이렇게 하려면 Nero 와 같은 CD/DVD 기록 프로그램을 사용합니다.

참조:

응급 복구 디스크 제작 135

응급 복구 디스크를 사용하여 컴퓨터 부팅 136

응급 복구 디스크 제작

응급 복구 디스크를 제작한다는 것은 최신 안티 바이러스 데이터베이스와 구성 파일이 있는 디스크 이미지(ISO 파일)를 생성한다는 의미입니다.

새 파일 생성의 기반이 되는 소스 디스크 이미지는 카스퍼스키 랩 서버에서 다운로드하거나 로컬 소스에서 복사할 수 있습니다.

마법사에 의해 생성된 이미지 파일은 "*Documents and Settings₩All Users₩Application Data₩Kaspersky Lab₩AVP80₩Data₩Rdisk₩*" 폴더(또는 Microsoft Vista 의 경우 "*ProgramData₩Kaspersky Lab₩AVP80₩Data₩Rdisk₩*")에 *rescuecd.iso* 라는 이름으로 저장됩니다. 마법사가 지정된 폴더에서 이전에 만들어진 이미지 파일을 탐지한 경우 **이전에 만들어진 ISO 파일** 상자를 체크하고 3 단계 – 이미지 업데이트로 이동하여 이전에 만들어진 이미지 파일을 원본 디스크 이미지로 사용할 수 있습니다. 마법사가 이미지 파일을 탐지하지 않은 경우 이 상자를 사용할 수 없습니다.

응급 복구 디스크는 일련의 상자(단계)로 구성된 마법사에 의해 생성됩니다. 단계는 **뒤로** 및 **다음** 버튼을 이용해 탐색할 수 있습니다. **완료 예상 시간** 버튼을 누르면 마법사의 활동이 완료됩니다. 어느 단계에서나 마법사를 중지하려면 **취소** 버튼을 사용하십시오.

참조:

응급 복구 디스크 134

응급 복구 디스크를 사용하여 컴퓨터 부팅 136

응급 복구 디스크를 사용하여 컴퓨터 부팅

바이러스 공격으로 인해 운영 체제를 부팅할 수 없을 경우 응급 복구 디스크를 사용하십시오.

운영 체제를 로드하려면 부트 디스크 이미지 파일(.iso)이 필요합니다. 카스퍼스키 랩 서버에서 ISO 파일을 다운로드하거나 기존의 파일을 업데이트할 수 있습니다.

응급 복구 디스크 기능에 대해 자세히 살펴보겠습니다. 디스크를 로드할 때 다음과 같은 작업이 수행됩니다:

1. 컴퓨터 하드웨어 자동 탐지
2. 하드 드라이브에서 파일 시스템 검색. 탐지된 파일 시스템에는 *C*로 시작하는 이름이 할당됩니다.

   하드 드라이브와 이동식 장치에 할당된 이름은 운영 체제에서 할당한 이름과 일치하지 않을 수 있습니다.

   로드 중인 컴퓨터의 운영 체제가 절전 모드이거나 잘못된 종료로 인해 파일 시스템이 *불완전한* 상태인 경우 파일 시스템을 마운트할지, 또는 컴퓨터를 다시 시작할지 선택할 수 있는 메시지가 표시됩니다.

   파일 시스템을 마운트하면 파일 시스템이 손상될 수 있습니다.
3. Microsoft Windows Swap 파일 *pagefile.sys* 검색. 이 파일이 없으면 가상 메모리의 용량이 RAM 크기에 의해 제한됩니다.
4. 현지화 언어 선택. 일정 시간이 경과할 때까지 언어를 선택하지 않으면 영어가 기본 언어로 설정됩니다.
5. 안티 바이러스 데이터베이스, 리포트, 격리저장소 및 추가 파일을 위한 폴더 검색(생성). 기본적으로, 감염된 컴퓨터에 설치된 카스퍼스키 랩 프로그램의 폴더(Microsoft Windows Vista 의 경우 *ProgramData/Kaspersky Lab/AVP8*, Microsoft Windows 초기 버전의 경우 *Documents and Settings/All Users/Application Data/Kaspersky Lab/AVP8*)가 사용됩니다. 그러한 프로그램 폴더를 찾을 수 없을 경우 생성 시도가 이루어집니다. 그러한 폴더가 없을 뿐 아니라 만들 수도 없는 경우에는 시스템 디스크에 *kl.files* 폴더가 생성됩니다.
6. 로드 중인 컴퓨터의 시스템 파일에 있는 데이터를 기반으로 네트워크 연결 구성 시도
7. 그래픽 서브시스템 로드 및 카스퍼스키 응급 복구 디스크 시작

시스템 응급 복구 모드에서는 바이러스 검사 작업, 로컬 소스에서 데이터베이스 업데이트, 롤백 업데이트 및 통계 보기만 가능합니다.

- *감염된 컴퓨터의 운영 체제를 로드하려면 다음과 같이 하십시오:*

1. BIOS 설정에서 CD/DVD-ROM 에서 부팅할 수 있습니다(자세한 내용은 컴퓨터에 설치된 마더보드 설명서 참조).
2. 응급 복구 디스크 이미지 파일이 있는 CD/DVD 를 감염된 컴퓨터의 CD/DVD 드라이브에 삽입합니다.

3. 컴퓨터를 다시 시작합니다.

위에 설명된 알고리즘에 따라 부팅을 계속합니다. 응급 복구 디스크의 기능에 대한 자세한 내용은 카스퍼스키 응급 복구 디스크 도움말을 참조하십시오

참조:

응급 복구 디스크 134

응급 복구 디스크 제작 135

브라우저 구성

브라우저 보안 마법사는 보안 관점에서 Microsoft Internet Explorer 설정을 분석합니다. 사용자가 선택한 설정 또는 기본값 설정 중 일부는 보안 문제를 야기할 수 있습니다.

브라우저 보안 마법사는 브라우저에 대한 최신 소프트웨어 업데이트가 설치되었는지, 침입자가 컴퓨터를 손상시키는 데 사용할 수 있는 잠재적 취약점이 설정에 포함되지 않았는지 확인합니다. 분석되는 개체의 예는 다음과 같습니다:

- **Microsoft Internet Explorer 캐시**. 캐시에는 기밀 데이터가 포함되어 있으며 캐시를 통해 사용자가 방문한 웹사이트 목록도 얻을 수 있습니다. 또한 일부 악성 개체는 디스크를 검사하는 동안 캐시를 검사하여 침입자가 사용자의 이메일 주소를 얻을 수 있습니다. 브라우저를 닫을 때마다 캐시를 삭제하는 것이 좋습니다.
- **알려진 파일 형식의 파일 확장명 표시**. Windows 탐색기에는 파일 확장명을 숨기는 옵션이 있습니다. 많은 악성 프로그램 개체가 이중 확장명을 사용하며 이 경우 사용자는 실제 확장명 없이 파일 이름의 일부만 볼 수 있습니다. 이 방법은 침입자가 종종 사용합니다. 알려진 파일 형식의 파일 확장명 표시를 사용하는 것이 좋습니다.
- **신뢰하는 사이트 목록**. 악성 프로그램 개체는 침입자의 웹사이트 링크를 이 목록에 추가할 수 있습니다.

진단을 시작하기 전에 Microsoft Internet Explorer 창을 모두 닫아야 합니다.

검토가 완료되면 마법사는 정보를 분석하여 즉각적인 주의가 필요한 보안 문제를 일으키는 브라우저 설정이 있는지 평가합니다. 그런 다음 문제를 해결하기 위해 수행할 처리 방법 목록을 작성합니다. 이러한 작업은 탐지되는 문제의 위험도에 따라 카테고리로 구분됩니다.

마법사가 완료되면 리포트가 생성되어 카스퍼스키 랩에 전송되고 여기서 분석이 이루어집니다.

일부 설정은 특정 사이트(예: ActiveX 컨트롤 사용 사이트)를 표시하는 데 문제를 일으킬 수 있습니다. 그 경우 해당 사이트를 신뢰 구역에 추가하면 문제를 해결할 수 있습니다.

마법사는 **뒤로** 및 **다음** 버튼을 사용하여 이동하는 일련의 화면(단계)으로 구성됩니다. 작업이 완료된 후 마법사를 닫으려면 **끝내기** 버튼을 사용합니다. 어느 단계에서나 마법사를 중지하려면 **취소** 버튼을 사용하십시오.

- *마법사를 시작하려면 다음과 같이 하십시오:*

  1. 메인 프로그램 창을 엽니다.

  2. 창 왼쪽에서 **보안 서비스+** 섹션을 선택하고 **브라우저 설정 최적화** 버튼을 누릅니다.

감염 후 복원

시스템 복구 마법사는 시스템에서 악성 개체의 작업 추적을 제거합니다. 컴퓨터를 치료한 후에는 이 마법사를 실행하여 감염으로 인한 모든 보안위협과 손상을 수정하는 것이 좋습니다. 또한 컴퓨터의 감염이 의심되는 경우에도 이 마법사를 사용할 수 있습니다.

시스템 복구 마법사는 네트워크 접근 차단, 알려진 파일 형식 확장자 변경, 툴바 차단과 같은 시스템 변경이 있는지 확인합니다. 시스템 손상은 악성 프로그램의 작업과 시스템 오류는 물론 시스템 최적화 프로그램의 잘못된 작동으로도 발생할 수 있습니다.

검토가 완료되면 마법사는 정보를 분석하여 즉각적인 주의가 필요한 시스템 손상이 있는지 평가합니다. 검토 결과에 따라 문제를 제거하는 데 필요한 처리 방법 목록이 생성됩니다. 이러한 작업은 탐지되는 문제의 위험도에 따라 카테고리로 구분됩니다.

마법사는 **뒤로** 및 **다음** 버튼을 사용하여 이동하는 일련의 화면(단계)으로 구성됩니다. 작업이 완료된 후 마법사를 닫으려면 **끝내기** 버튼을 사용합니다. 어느 단계에서나 마법사를 중지하려면 **취소** 버튼을 사용하십시오.

- *마법사를 시작하려면 다음과 같이 하십시오:*

  1. 메인 프로그램 창을 엽니다.

  2. 창 왼쪽에서 **보안 서비스+** 섹션을 선택하고 **Microsoft Windows 설정 최적화** 버튼을 누릅니다.

개인정보보호 마법사

컴퓨터 사용자 작업의 대부분은 시스템에 기록됩니다. 다음과 같은 데이터가 저장됩니다:

- 정보를 포함한 사용 내역:
  - 방문한 웹사이트
  - 실행한 프로그램
  - 검색 요청
  - 여러 프로그램에서 파일 열기/저장

- Microsoft Windows 시스템 로그 레코드.
- 임시 파일 등

사용자 활동에 대한 이러한 모든 정보 출처에는 기밀 데이터(예: 암호)가 포함되어 침입자가 이를 분석할 수 있습니다. 사용자는 지식이 부족하여 이런 방식으로 정보를 훔치는 것을 방지하지 못하는 경우가 많습니다.

카스퍼스키 안티 바이러스에는 **개인정보보호 마법사**가 포함되어 있습니다. 이 마법사는 시스템에서 사용자 활동을 추적하는 것은 물론 사용자 활동에 대한 정보를 저장하기 쉽게 만드는 운영 체제 설정을 검색합니다.

시스템에서 사용자 활동에 대한 정보는 지속적으로 저장됩니다. 파일 실행이나 문서 열기 등이 모두 기록되며 Microsoft Windows 시스템 로그에는 시스템에서 발생하는 많은 이벤트가 기록됩니다. 이러한 이유로 **개인정보보호 마법사**를 반복해서 실행하면 이전 마법사 실행 시 정리하지 못한 활동 추적을 탐지할 수 있습니다. Microsoft Windows 로그 파일과 같은 일부 파일은 마법사에서 삭제하려고 할 때 시스템에서 사용되고 있을 수 있습니다. 이러한 파일을 삭제하기 위해 마법사에서는 시스템을 다시 시작하도록 제안합니다. 그러나 다시 시작 중 이러한 파일이 재생성되어 활동 추적으로 다시 탐지될 수 있습니다.

마법사는 **뒤로** 및 **다음** 버튼을 사용하여 이동하는 일련의 화면(단계)으로 구성됩니다. 작업이 완료된 후 마법사를 닫으려면 **끝내기** 버튼을 사용합니다. 어느 단계에서나 마법사를 중지하려면 **취소** 버튼을 사용하십시오.

- *마법사를 시작하려면 다음과 같이 하십시오:*

1. 메인 프로그램 창을 엽니다.
2. 창 왼쪽에서 **보안 서비스+** 섹션을 선택하고 **컴퓨터 사용 내역 지우기** 버튼을 누릅니다.

리포트

각 카스퍼스키 안티 바이러스 구성요소 작동과 각 바이러스 검사 및 업데이트 작업 성능은 리포트에 기록됩니다.

리포트 작업 시에는 다음 처리 방법을 수행할 수 있습니다:

- 이벤트 리포트를 보려는 구성요소 또는 작업 선택
- 데이트 그룹화 관리 및 시화면에 데이터 표
- 스케줄 생성. 이 스케줄에 따라 카스퍼스키 안티 바이러스에서 리포트 준비에 대해 알립니다.
- 리포트를 생성하려는 이벤트 유형 선택
- 통계 정보를 화면에 표시할 방법 선택 – 표 또는 그래픽 보기
- 파일로 리포트 저장
- 복잡한 필터링 조건
- 시스템에서 발생하고 카스퍼스키 안티 바이러스에서 처리된 이벤트 검색

참조:

리포트를 생성할 구성요소 또는 작업 선택 141

리포트에서 정보 그룹 표시 관리 141

리포트 준비 알림 142

이벤트 유형 선택 142

화면에 데이터 표시 143

통계 정보에 대한 표 또는 그래픽 프레젠테이션 144

파일로 리포트 저장 145

복잡한 필터링 사용 145

이벤트 검색 146

리포트를 생성할 구성요소 또는 작업 선택

각 카스퍼스키 안티 바이러스 구성요소 작동 중 또는 작업(예: 파일 안티 바이러스, 업데이트 등) 실행 중 발생한 이벤트에 대한 정보를 얻을 수 있습니다.

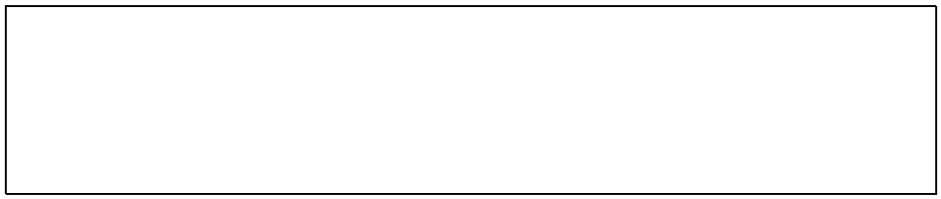
- *특정 구성요소 또는 작업에 대한 리포트를 생성하는 방법은 다음과 같습니다.*

  1. 메인 프로그램 창을 열고 창 상단의 **리포트** 링크를 누릅니다.
  2. 열리는 창에서 **리포트** 탭 아래 있는 **상세한 리포트** 버튼을 누릅니다.
  3. 열리는 창의 왼쪽 드롭다운 목록에서 리포트를 생성할 구성요소 또는 작업을 선택합니다. **실시간 감시** 항목을 선택하면 모든 실시간 감시 구성요소에 대한 리포트가 생성됩니다.

리포트에서 정보 그룹 표시 관리

몇 가지 특성을 사용하여 리포트에서 정보가 그룹으로 표시되는 방법을 관리할 수 있습니다. 특성 집합은 각 카스퍼스키 안티 바이러스 구성요소 및 작업에 따라 다릅니다. 다음과 같은 옵션을 선택할 수 있습니다:

- **그룹으로 표시 안함**. 모든 이벤트가 표시됩니다.
- **작업 그룹으로 표시**. 데이터가 카스퍼스키 안티 바이러스 구성요소에서 수행한 작업에 따라 그룹으로 표시됩니다.
- **프로그램 그룹으로 표시**. 데이터가 시스템에서 활동이 나타나고 카스퍼스키 안티 바이러스에서 처리된 프로그램에 따라 그룹 표시됩니다.
- **결과 그룹으로 표시**. 데이터가 검사 또는 개체 처리 결과에 따라 그룹으로 표시됩니다.



리포트에서 정보를 그룹으로 표시할 특성

특정 정보를 빠르게 얻고 그룹 표시 크기를 줄이도록 키워드 검색 조건이 제공됩니다. 검색 조건을 지정할 수도 있습니다.

- *특정 특성에 따라 그룹 표시를 사용하는 방법은 다음과 같습니다:*

  1. 메인 프로그램 창을 열고 창 상단의 **리포트** 링크를 누릅니다.
  2. 열리는 창에서 **리포트** 탭 아래 있는 **상세한 리포트** 버튼을 누릅니다.

3. 열리는 창의 드롭다운 메뉴에서 그룹 표시 특성을 선택합니다.

리포트 준비 알림

카스퍼스키 안티 바이러스가 리포트 준비 알림을 보내는 스케줄을 생성할 수 있습니다.

- *알림 스케줄을 생성하는 방법은 다음과 같습니다:*

1. 메인 프로그램 창을 열고 창 상단의 **리포트** 링크를 누릅니다.
2. 열리는 창에서 **리포트** 탭 아래 있는 **리포트 작성 완료 알림** 상자를 체크합니다. 사전 설정된 시간 값을 갖는 링크를 누릅니다.
3. 열리는 **리포트 스케줄** 창에서 스케줄을 생성합니다.

이벤트 유형 선택

실시간 감시 구성요소 활동 중에 발생하는 모든 중요 이벤트, 검사 작업 실행 또는 프로그램 데이터베이스 업데이트에 대한 전체 목록이 리포트에 기록됩니다. 리포트에 기록할 이벤트 유형을 선택할 수 있습니다.

이벤트는 다음 유형으로 분류할 수 있습니다.

- *매우 중요한 이벤트*. 카스퍼스키 안티 바이러스 작동에 문제가 있거나 컴퓨터 감시에 취약점이 있는 것을 나타내는 매우 중요한 이벤트입니다. 예를 들어 바이러스 탐지 또는 작동 오류가 포함됩니다.
- *중요한 이벤트*. 카스퍼스키 안티 바이러스 작동에 중요한 상황을 나타내므로 항상 주의를 기울여야 하는 이벤트입니다. 예를 들어 **종료** 이벤트가 포함됩니다.

이벤트 유형 선택

모든 이벤트 항목을 선택한 경우 모든 이벤트가 리포트에 표시됩니다. 단, **리포트 및 저장소** 설정의 **리포트** 섹션에서 해당 상자를 체크해야 합니다. 이 상자를 통해 중요하지 않은 이벤트와 파일 시스템 및 레지스트리 이벤트 레코드를 리포트에 기록할 수 있습니다. 이 상자를 체크하지 않으면 드롭다운 이벤트 유형 선택 목록 근처에 경고 아이콘과 **이 기능 사용 안함** 링크가 표시됩니다. 해당 상자를 체크하려면 이 링크를 사용하여 리포트 설정 창으로 이동합니다.

- *특정 이벤트 유형에 대한 리포트를 생성하는 방법은 다음과 같습니다.*

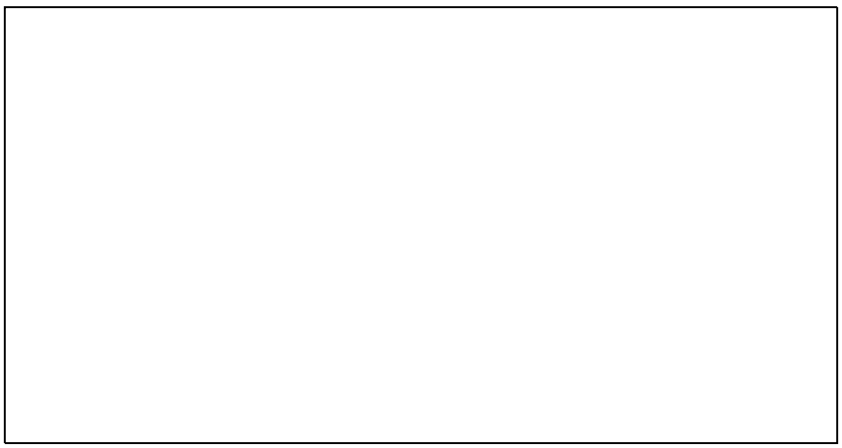
1. 메인 프로그램 창을 열고 창 상단의 **리포트** 링크를 누릅니다.

2. 열리는 창에서 **리포트** 탭 아래 있는 **상세한 리포트** 버튼을 누릅니다.

3. 열리는 창의 드롭다운 메뉴에서 이벤트 유형을 선택합니다. 모든 이벤트에 대한 리포트를 생성해야 하는 경우 **모든 이벤트** 값을 선택합니다.

화면에 데이터 표시

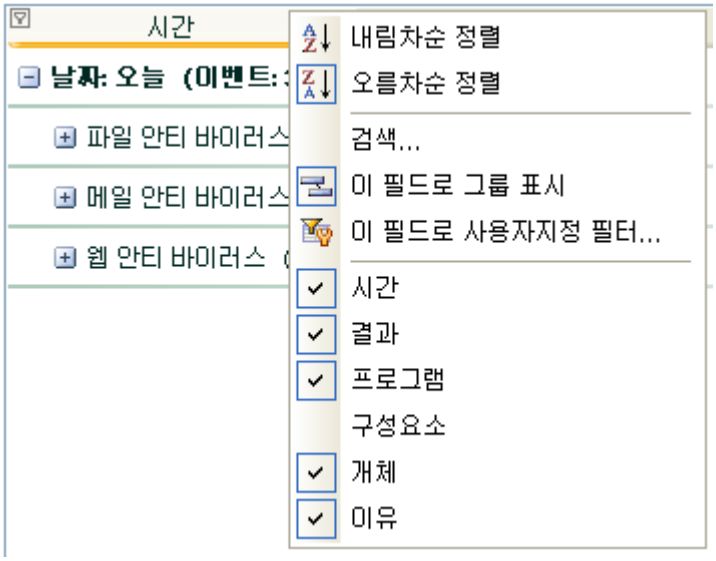
리포트에 포함되는 이벤트는 표로 표시됩니다. 제한 조건을 지정하여 데이터 집합을 생성하고 정보를 필터링할 수 있습니다. 이렇게 하려면 제한을 적용할 표 열 제목의 왼쪽 영역을 누릅니다. 드롭다운 목록에 가능한 제한 조건 값이 표시됩니다(예: **시간** 열의 경우 **어제**, **개체** 열의 경우 **이메일 메시지** 등). 각 열에 대해 필요한 값을 선택합니다. 목록에서 가장 적합한 값을 선택하면 됩니다. 지정한 제한 조건에 따라 쿼리가 수행됩니다. 모든 데이터를 보려면 제한 목록에서 **모두** 항목을 선택합니다.



제한 조건 지정

또한 이전 이벤트에 대한 데이터를 선택할 간격 형태로 복잡한 검색 설정을 지정할 수 있습니다. 이렇게 하려면 제한 드롭다운 목록에서 **사용자지정** 항목을 선택합니다. 열리는 창에서 필요한 간격을 지정합니다.

마우스 오른쪽 메뉴를 통해 특성에 접근하여 그룹화 및 이벤트 쿼리를 수행하면 리포트를 간편하게 생성할 수 있습니다.



마우스 오른쪽 메뉴

제한을 지정하는 방법은 다음과 같습니다.

1. 메인 프로그램 창을 열고 창 상단의 **리포트** 링크를 누릅니다.
2. 열리는 창에서 **리포트** 탭 아래 있는 **상세한 리포트** 버튼을 누릅니다.
3. 열리는 창에서 제한을 적용할 표 열 제목의 왼쪽 영역을 누릅니다. 드롭다운 목록에서 필요한 제한을 선택합니다. **사용자지정** 항목을 선택하면 복잡한 필터링 조건을 지정할 수 있습니다.

- *표 열을 숨기거나 표시하는 방법은 다음과 같습니다*

4. 메인 프로그램 창을 열고 창 상단의 **리포트** 링크를 누릅니다.
5. 열리는 창에서 **리포트** 탭 아래 있는 **상세한 리포트** 버튼을 누릅니다.
6. 열리는 창에서 표 열 제목의 오른쪽 영역을 마우스 오른쪽 버튼으로 누릅니다. 표 열을 숨기려면 마우스 오른쪽 메뉴에서 해당 이름 옆에 있는 상자를 체크해제 합니다.

통계 정보에 대한 표 또는 그래픽 표시

리포트 창 하단에는 카스퍼스키 안티 바이러스에서 선택한 구성요소 동작 또는 작업에 대한 통계가 포함됩니다. 통계를 검토하고 표시 방법을 그래픽 형태(구성요소의 경우) 또는 표 보기 중에 선택할 수 있습니다. 표시 방법은 창 상단의 및 버튼을 사용하여 선택합니다. 통계는 현재 날짜와 카스퍼스키 안티 바이러스를 컴퓨터에 설치한 이후의 전체 기간에 대해 표시됩니다.

- *통계 표시 방법을 선택하는 방법은 다음과 같습니다.*

  1. 메인 프로그램 창을 열고 창 상단의 **리포트** 링크를 누릅니다.
  2. 열리는 창에서 **리포트** 탭 아래 있는 **상세한 리포트** 버튼을 누릅니다.
  3. 열리는 창에서 통계를 보려는 프로그램 구성요소를 선택하고 창 상단의 및 버튼을 사용합니다.

파일로 리포트 저장

생성된 리포트를 파일로 저장할 수 있습니다.

- *생성된 리포트를 파일로 저장하는 방법은 다음과 같습니다.*

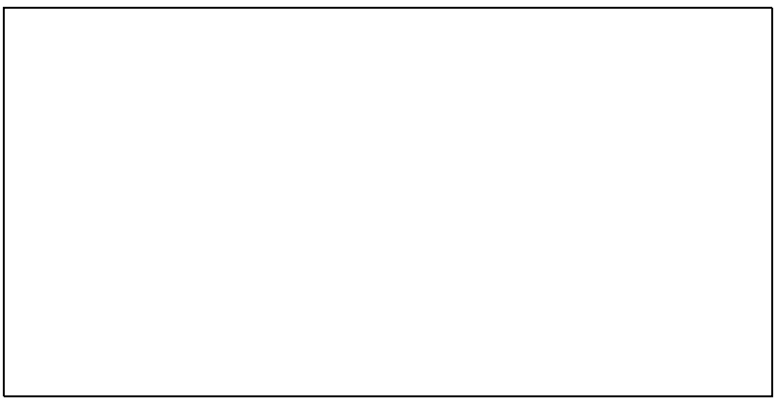
  1. 메인 프로그램 창을 열고 창 상단의 **리포트** 링크를 누릅니다.
  2. 열리는 창에서 **리포트** 탭 아래 있는 **상세한 리포트** 버튼을 누릅니다.
  3. 열리는 창에서 필요한 리포트를 생성하고 **저장** 버튼을 누릅니다.
  4. 열리는 창에서 리포트 파일을 저장할 폴더를 선택하고 파일 이름을 입력합니다.

복잡한 필터링 사용

사용자지정 필터 창(아래 그림 참조)에서는 복잡한 데이터 필터링 조건을 지정할 수 있습니다. 모든 표 열에 대해 데이터 검색 조건을 지정할 수 있습니다. 예를 들어 창에서 **시간** 열을 사용하여 작업하는 절차를 살펴보겠습니다.

복잡한 필터를 사용하는 데이터 쿼리는 논리 결합(논리 AND) 함수와 논리 분리(논리 OR) 함수를 기반으로 쿼리를 제어합니다.

쿼리 제한(이 경우 "시간")은 창 오른쪽 칸에 표시됩니다. 시간을 지정하는 데 키보드의 화살표 키를 사용할 수 있습니다. 드롭다운 목록 **필터 값 지정**에서 이벤트 쿼리의 조건(예: **다음보다 큼**, 즉 오른쪽 칸에 지정한 값 초과)을 선택할 수 있습니다.



복잡한 필터링 조건 지정

데이터 쿼리가 지정한 조건을 모두 만족하도록 하려면 **그리고**를 선택합니다. 두 조건 중 하나만 필요한 경우 **또는**을 선택합니다.

몇몇 데이터 유형의 경우 검색 간격 제한이 숫자 또는 임시 값이 아니라 단어입니다(예: **결과** 열에 **확인** 값이 표시될 수 있음). 이러한 경우 제한으로 지정된 단어가 다른 단어 조건과 사전순으로 비교됩니다.

- *복잡한 필터링 조건을 지정하는 방법은 다음과 같습니다.*

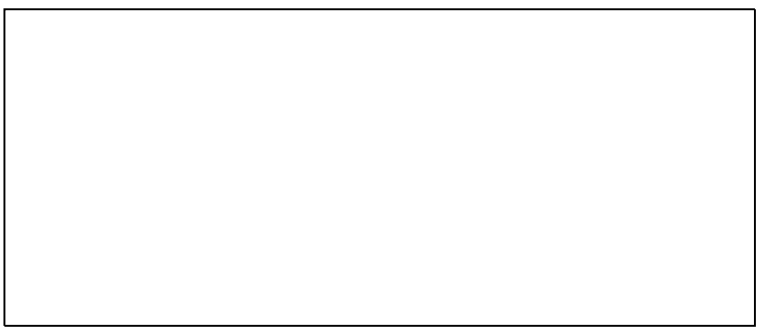
1. 메인 프로그램 창을 열고 창 상단의 **리포트** 링크를 누릅니다.
2. 열리는 창에서 **리포트** 탭 아래 있는 **상세한 리포트** 버튼을 누릅니다.
3. 열리는 창에서 복잡한 필터링 조건을 지정하려는 표 열의 왼쪽 영역을 누릅니다. 드롭다운 메뉴에서 **사용자지정** 항목을 선택합니다. 또한 표의 필요한 열을 마우스 오른쪽 버튼으로 눌러 표시되는 마우스 오른쪽 메뉴에서 **이 필드로 사용자지정 필터** 항목을 선택할 수도 있습니다.
4. **사용자지정 필터** 창에서 필요한 필터 조건을 지정합니다.

이벤트 검색

이벤트 검색 창(아래 그림 참조)에서는 시스템에서 발생하고 카스퍼스키 안티 바이러스에서 처리된 이벤트를 검색할 수 있습니다.

아래에는 이 창 작업 시 사용되는 원리를 설명합니다.

- **찾을 내용** 칸은 키워드(예: explorer)를 입력하는 데 사용됩니다. 검색을 시작하려면 **다음 찾기** 버튼을 누릅니다. 요청한 데이터를 검색하는 데는 약간의 시간이 걸릴 수 있습니다. 검색이 완료되면 입력한 키워드와 관련된 이벤트가 표시됩니다. **모두 표시** 버튼을 누르면 검색 키워드와 일치하는 모든 찾은 항목이 선택됩니다.
- **열** 칸은 키워드 검색을 수행할 표 열을 선택하는 데 사용됩니다. 검색할 열을 선택하면 검색에 소요되는 시간을 절약할 수 있습니다(**모두** 값을 선택하지 않는 한).



이벤트 검색

대소문자를 구분하여 검색하려면 ☑ **대/소문자 구분** 상자를 체크합니다. ☑ **온전한 단어** 상자를 체크하면 단어 단위로 검색이 제한됩니다.

- *이벤트 검색을 사용하는 방법은 다음과 같습니다.*

    1. 메인 프로그램 창을 열고 창 상단의 **리포트** 링크를 누릅니다.

    2. 열리는 창에서 **리포트** 탭 아래 있는 **상세한 리포트** 버튼을 누릅니다.

    3. 열리는 창에서 표 열 제목의 오른쪽 영역을 마우스 오른쪽 버튼으로 누릅니다. 마우스 오른쪽 메뉴에서 **검색** 항목을 선택합니다.

    4. 열리는 **검색** 창에서 검색 조건을 지정합니다.

알림

카스퍼스키 안티 바이러스 런타임 이벤트가 발생하면 특별한 알림 메시지가 표시됩니다. 컴퓨터 보안에 대한 이벤트의 중요도에 따라 다음 3 가지 종류의 알림이 표시됩니다.

- **경보**. 악성 개체 또는 위험 활동이 시스템에서 감지되는 등 중요한 이벤트가 발생한 경우에 표시됩니다. 이 경우 해당 보안위협을 어떻게 처리할지 즉시 결정해야 합니다. 이 유형의 알림 창은 빨간색으로 표시됩니다.

- **경고**. 감염 위험 파일 또는 의심스러운 활동이 시스템에서 감지된 경우와 같이 잠재적으로 위험할 수 있는 이벤트가 발생한 경우 표시됩니다. 사용자는 이것의 위험성이 어느 정도인지 결정해야 합니다. 이 유형의 알림 창은 노란색으로 표시됩니다.

- **정보**. 이 알림에서는 중요하지 않은 이벤트에 대한 정보를 제공하며 초록색 창으로 나타납니다.

알림 창은 다음과 같이 4 가지로 구성됩니다.

1. *창 헤더*. 알림 창 헤더에는 권한 요청, 의심스러운 활동, 새로운 네트워크, 경보, 바이러스 등 이벤트에 대한 간단한 설명이 포함되어 있습니다.

2. *이벤트 설명*. 이벤트 설명 섹션에는 이벤트를 발생시킨 프로그램의 이름, 탐지된 보안위협의 이름, 탐지된 네트워크 연결의 설정 등 알림이 나타난 이유에 대한 자세한 설명이 표시됩니다.

3. *처리 선택 영역*. 이 섹션에서는 해당 이벤트에 대해 수행할 수 있는 처리 중 하나를 선택할 수 있습니다. 처리 옵션은 이벤트 유형에 따라 **치료**, **삭제**, **건너뛰기**(바이러스가 탐지된 경우), **허락**, **차단**(프로그램에서 잠재적으로 위험한 처리를 실행할 권한을 요청한 경우) 등으로 나눠집니다. 카스퍼스키 랩 전문가가 권장하는 처리는 굵은 글씨체로 표시됩니다.

   허락 또는 **차단**을 선택한 경우 *처리 적용 모드*를 선택할 수 있는 창이 열립니다. **허락**의 경우 다음 모드 중 하나를 선택할 수 있습니다.

   - **항상 허락**. 시스템 리소스에 대한 프로그램 액세스의 규칙을 변경하여 프로그램의 활동을 허락하려면 이 옵션을 선택합니다.

   - **지금 허락**. 프로그램 세션 동안 탐지된 모든 유사 이벤트에 대해 지정한 처리를 적용하려면 이 옵션을 선택합니다. 프로그램 세션은 프로그램이 시작된 순간부터 종료되거나 다시 시작되는 순간까지입니다.

   - **신뢰하는 그룹으로 지정**. 프로그램을 **신뢰하는** 그룹으로 이동하려면 이 옵션을 선택합니다.

   차단의 경우 다음 모드 중 하나를 선택할 수 있습니다.

   - **항상 차단**. 시스템 리소스에 대한 프로그램 액세스의 규칙을 변경하여 프로그램의 활동을 차단하려면 이 옵션을 선택합니다.

- **지금 차단.** 프로그램 세션 동안 탐지된 모든 유사 이벤트에 대해 지정한 처리를 적용하려면 이 옵션을 선택합니다. 프로그램 세션은 프로그램이 시작된 순간부터 종료되거나 다시 시작되는 순간까지입니다.
- **끝내기**. 프로그램의 작업을 중단하려면 이 옵션을 선택합니다.

4. *추가 처리 선택 영역*. 이 섹션을 사용하여 추가 처리를 선택할 수 있습니다.
   - **제외에 추가**. 탐지된 개체가 악성이 아니라고 확신하는 경우 해당 개체를 신뢰하는 영역에 추가하여 개체를 사용할 때 프로그램에서 정상적인 개체를 탐지하는 현상을 방지하는 것이 좋습니다.
   - **모든 개체에 적용**. 유사한 상황에서 상태가 동일한 모든 개체에 지정된 처리를 적용하려면 이 확인란을 선택합니다.

참조:

악성 개체 탐지 149

개체 치료 불가 150

고급 치료 기술 필요 151

트래픽에서 위험 개체 탐지 151

감염의심 개체 탐지 151

시스템에서 위험 활동 탐지 152

숨겨진 프로세스 탐지 153

시스템 레지스트리 접근 시도 탐지 154

피싱 공격 탐지 154

감염의심 링크 탐지 155

잘못된 인증서 탐지 155

악성 개체 탐지

파일 안티 바이러스, 메일 안티 바이러스 또는 바이러스 검사를 통해 악성 코드가 탐지된 경우 특별 알림 팝업이 표시됩니다.

내용은 다음과 같습니다.

- 카스퍼스키 랩 바이러스 진단 명에 나열된 보안위협 형태(예: *바이러스*, *트로이목마*) 및 악성 개체의 이름. 위험 개체의 이름은 컴퓨터에서 탐지된 보안위협 형태에 대한 상세한 정보를 찾을 수 있는 www.viruslist.com 링크로 제공됩니다.

- 악성 개체의 전체 이름 및 경로.

개체에 대해 다음 응답 중 하나를 선택해야 합니다.

- **치료** - 악성 개체를 치료하려고 시도합니다. 개체 또는 유사한 것에 대한 복원 필요성이 제기되는 경우 치료하기 전에 개체의 백업 복사본이 생성됩니다.

- **삭제** - 악성 개체를 삭제합니다. 개체 또는 유사한 것에 대한 복원 필요성이 제기되는 경우 삭제하기 전에 개체의 백업 복사본이 생성됩니다.

- **건너뛰기** - 개체에 대한 접근은 차단하지만 처리 방법은 수행하지 않고 리포트에 관련 정보를 기록합니다.

  나중에 리포트 창에서 건너뛴 악성 개체로 다시 돌아갈 수 있습니다. 그러나 이메일에서 탐지된 개체에 대한 처리는 연기할 수 없습니다.

감시 구성요소 또는 작업 동작의 현재 세션에서 탐지된 모든 동일 상태의 개체에 선택한 처리 방법을 적용하려면 ☑ **모두 적용** 상자를 체크하십시오. 현재 세션은 구성요소가 시작된 후부터 중지되거나 프로그램이 다시 시작될 때까지의 시간 또는 바이러스 검사가 시작된 후부터 완료될 때까지의 시간입니다.

개체 치료 불가

악성 개체의 치료가 불가능한 경우가 종종 있습니다. 악성 코드를 삭제하여도 파일의 신뢰성을 회복하기 어려울 정도로 손상된 경우가 해당될 수 있습니다. 트로이목마와 같은 여러 유형의 위험 개체에는 치료 절차를 적용할 수 없습니다.

이 경우 다음 내용이 포함된 특별 알림 팝업이 표시됩니다.

- 카스퍼스키 랩 바이러스 진단 명에 나열된 보안위협 형태(예: *바이러스*, *트로이목마*) 및 악성 개체의 이름. 위험 개체의 이름은 컴퓨터에서 탐지된 보안위협 형태에 대한 상세한 정보를 찾을 수 있는 www.viruslist.com 링크로 제공됩니다.

- 악성 개체의 전체 이름 및 경로.

개체에 대해 다음 응답 중 하나를 선택해야 합니다.

- **삭제** - 악성 개체를 삭제합니다. 개체 또는 유사한 것에 대한 복원 필요성이 제기되는 경우 삭제하기 전에 개체의 백업 복사본이 생성됩니다.

- **건너뛰기** - 개체에 대한 접근은 차단하지만 처리 방법은 수행하지 않고 리포트에 관련 정보를 기록합니다.

  나중에 리포트 창에서 건너뛴 악성 개체로 다시 돌아갈 수 있습니다. 그러나 이메일에서 탐지된 개체에 대한 처리는 연기할 수 없습니다.

감시 구성요소 또는 작업 동작의 현재 세션에서 탐지된 모든 동일 상태의 개체에 선택한 처리 방법을 적용하려면 ☑ **모두 적용** 상자를 체크하십시오. 현재 세션은 구성요소가 시작된 후부터 중지되거나 프로그램이 다시 시작될 때까지의 시간 또는 바이러스 검사 작업이 시작된 후부터 완료될 때까지의 시간입니다.

고급 치료 기술 필요

시스템에서 처리되지 않은 보안위협(예: RAM 또는 자동 시작 개체의 악성 프로세스)이 탐지된 경우 고급 치료 절차를 수행할지 확인하는 팝업 메시지가 표시됩니다.

카스퍼스키 랩 전문가는 고급 치료 절차를 수행할 것을 강력하게 권장합니다. 그렇게 하려면 **확인** 버튼을 누르십시오. 그러나 치료 절차가 완료되면 컴퓨터가 재시작되므로 치료 절차를 실행하기 전에 현재 작업을 저장하고 모든 프로그램을 종료하십시오.

치료 절차가 실행 중일 때는 이메일 클라이언트 또는 운영 체제 레지스트리 편집 세션을 시작할 수 없습니다. 컴퓨터를 재시작한 후 전체 바이러스 검사를 실행하는 것이 좋습니다.

트래픽에서 위험 개체 탐지

웹 안티 바이러스를 통해 트래픽에서 악성 개체가 탐지된 경우 화면에 특별 알림 팝업이 표시됩니다.

알림 내용은 다음과 같습니다.

- 카스퍼스키 랩 바이러스 진단 명에 나열된 보안위협 형태(예: *바이러스 변종*) 및 위험 개체의 이름. 위험 개체의 이름은 컴퓨터에서 탐지된 보안위협 형태에 대한 상세한 정보를 찾을 수 있는 www.viruslist.com 링크로 제공됩니다.
- 위험 개체의 전체 이름 및 웹페이지 경로.

개체에 대해 다음 응답 중 하나를 선택해야 합니다.

- **허락** - 개체를 계속 다운로드합니다.
- **차단** - 웹 리소스에서 개체 다운로드를 차단합니다.

감시 구성요소 또는 작업 동작의 현재 세션에서 탐지된 모든 동일 상태의 개체에 선택한 처리 방법을 적용하려면 ☑ **모두 적용** 상자를 체크하십시오. 현재 세션은 구성요소가 시작된 후부터 중지되거나 프로그램이 다시 시작될 때까지의 시간 또는 바이러스 검사가 시작된 후부터 완료될 때까지의 시간입니다.

감염의심 개체 탐지

파일 안티 바이러스, 메일 안티 바이러스 또는 바이러스 검사를 통해 알려지지 않은 바이러스의 코드 또는 알려진 바이러스의 변형된 코드가 포함된 개체가 탐지된 경우 특별 알림 팝업이 표시됩니다.

내용은 다음과 같습니다.

- 카스퍼스키 랩 바이러스 진단 명에 나열된 보안위협 형태(예: *바이러스*, *트로이목마*) 및 개체의 이름. 위험 개체의 이름은 컴퓨터에서 탐지된 보안위협 형태에 대한 상세한 정보를 찾을 수 있는 www.viruslist.com 링크로 제공됩니다.

- 개체의 전체 이름 및 경로.

개체에 대해 다음 응답 중 하나를 선택해야 합니다.

- **격리저장소** - 개체를 격리저장소로 이동합니다. 개체를 격리저장소에 놓으면 복사되는 것이 아니라 이동이 됩니다. 개체는 디스크 또는 이메일에서 삭제되고 격리저장소 폴더에 저장됩니다. 격리저장소의 파일은 특별한 형식으로 저장되며 위험하지 않습니다.

  업데이트된 보안위협 서명을 사용하여 나중에 격리저장소를 검사할 경우 개체의 상태가 변경될 수 있습니다. 예를 들어, 개체는 감염된 것으로 식별되어 업데이트된 데이터베이스로 처리할 수 있습니다. 그렇지 않으면 개체에 *감염되지 않음* 상태가 할당되어 복원할 수 있습니다.

  사용자가 직접 파일을 격리시킨 경우 후속 검사에서 감염되지 않은 것으로 판명되어도 상태는 검사 직후 *안전*으로 변경되지 않습니다. 파일을 격리시킨 후 일정 시간(최소 3일)이 경과한 후에 검사를 수행할 때만 상태가 변경됩니다.

- **삭제** - 개체를 삭제합니다. 개체 또는 유사한 것에 대한 복원 필요성이 제기되는 경우 삭제하기 전에 개체의 백업 복사본이 생성됩니다.

- **건너뛰기** - 개체에 대한 접근은 차단하지만 처리 방법은 수행하지 않고 리포트에 관련 정보를 기록합니다.

  나중에 리포트 창에서 건너뛴 개체로 다시 돌아갈 수 있습니다. 그러나 이메일에서 탐지된 개체에 대한 처리는 연기할 수 없습니다.

감시 구성요소 또는 작업 동작의 현재 세션에서 탐지된 모든 동일 상태의 개체에 선택한 처리 방법을 적용하려면 **모두 적용** 상자를 체크하십시오. 현재 세션은 구성요소가 시작된 후부터 중지되거나 프로그램이 다시 시작될 때까지의 시간 또는 바이러스 검사가 시작된 후부터 완료될 때까지의 시간입니다.

탐지된 개체가 악성이 아니라고 확신하는 경우 해당 개체를 신뢰하는 영역에 추가하여 개체를 사용할 때 프로그램에서 정상적인 개체를 탐지하는 현상을 방지하는 것이 좋습니다.

시스템에서 위험 활동 탐지

사전 방역을 통해 시스템에서 위험 프로그램 활동이 탐지된 경우 다음 내용이 포함된 특별 알림 팝업이 표시됩니다.

- 카스퍼스키 랩 바이러스 진단 명에 나열된 보안위협의 이름. 보안위협의 이름은 컴퓨터에서 탐지된 보안위협 형태에 대한 상세한 정보를 찾을 수 있는 www.viruslist.com 링크로 제공됩니다.

- 위험 활동을 시작한 프로세스 파일의 전체 이름 및 경로.

- 가능한 응답:

  - **격리저장소** - 프로세스를 종료하고 실행 파일을 격리저장소로 이동합니다. 개체를 격리저장소에 놓으면 복사되지 않고 이동만 됩니다. 격리저장소의 파일은 특별한 형식으로 저장되며 위험하지 않습니다.

    업데이트된 보안위협 서명을 사용하여 나중에 격리저장소를 검사할 경우 개체의 상태가 변경될 수 있습니다. 예를 들어, 개체는 감염된 것으로 식별되어 업데이트된 데이터베이스로 처리할 수 있습니다. 그렇지 않으면 개체에 *감염되지 않음* 상태가 할당되어 복원할 수 있습니다.

    사용자가 직접 파일을 격리시킨 경우 후속 검사에서 감염되지 않은 것으로 판명되어도 상태는 검사 직후 *안전*으로 변경되지 않습니다. 파일을 격리시킨 후 일정 시간(최소 3일)이 경과한 후에 검사를 수행할 때만 상태가 변경됩니다.

  - **종료** - 프로세스를 종료합니다.

  - **허락** - 프로세스를 실행합니다.

감시 구성요소 또는 작업 동작의 현재 세션에서 탐지된 모든 동일 상태의 개체에 선택한 처리 방법을 적용하려면 **모두 적용** 상자를 체크하십시오. 현재 세션은 구성요소가 시작된 후부터 중지되거나 프로그램이 다시 시작될 때까지의 시간 또는 바이러스 검사가 시작된 후부터 완료될 때까지의 시간입니다.

탐지된 프로그램이 위험하지 않은 경우 프로그램을 탐지할 때 카스퍼스키 안티 바이러스에서 정상적인 프로그램을 반복해서 탐지하지 않도록 해당 프로그램을 신뢰 구역에 추가할 것을 권장합니다.

숨겨진 프로세스 탐지

사전 방역을 통해 시스템에서 숨겨진 프로세스가 탐지된 경우 다음 내용이 포함된 특별 알림 팝업이 표시됩니다.

- 카스퍼스키 랩 바이러스 진단 명에 나열된 보안위협의 이름. 보안위협의 이름은 컴퓨터에서 탐지된 보안위협 형태에 대한 상세한 정보를 찾을 수 있는 www.viruslist.com 링크로 제공됩니다.

- 숨겨진 프로세스 파일의 전체 이름 및 경로.

- 가능한 응답:

  - **격리저장소** - 프로세스의 실행 파일을 격리저장소로 이동합니다. 개체를 격리저장소에 놓으면 복사되지 않고 이동만 됩니다. 격리저장소의 파일은 특별한 형식으로 저장되며 위험하지 않습니다.

    업데이트된 보안위협 서명을 사용하여 나중에 격리저장소를 검사할 경우 개체의 상태가 변경될 수 있습니다. 예를 들어, 개체는 감염된 것으로 식별되어 업데이트된 데이터베이스로 처리할 수 있습니다. 그렇지 않으면 개체에 *감염되지 않음* 상태가 할당되어 복원할 수 있습니다.

    사용자가 직접 파일을 격리시킨 경우 후속 검사에서 감염되지 않은 것으로 판명되어도 상태는 검사 직후 *안전*으로 변경되지 않습니다. 파일을 격리시킨 후 일정 시간(최소 3일)이 경과한 후에 검사를 수행할 때만 상태가 변경됩니다.

- **종료** - 프로세스를 종료합니다.
- **허락** - 프로세스를 실행합니다.

감시 구성요소 또는 작업 동작의 현재 세션에서 탐지된 모든 동일 상태의 개체에 선택한 처리 방법을 적용하려면 ☑ **모두 적용** 상자를 체크하십시오. 현재 세션은 구성요소가 시작된 후부터 중지되거나 프로그램이 다시 시작될 때까지의 시간 또는 바이러스 검사가 시작된 후부터 완료될 때까지의 시간입니다.

탐지된 프로그램이 위험하지 않은 경우 프로그램을 탐지할 때 카스퍼스키 안티 바이러스에서 정상적인 프로그램을 반복해서 탐지하지 않도록 해당 프로그램을 신뢰 구역에 추가할 것을 권장합니다.

시스템 레지스트리 접근 시도 탐지

사전 방역을 통해 시스템 레지스트리 키에 접근하려는 시도가 탐지된 경우 다음 내용이 포함된 특별 알림 팝업이 표시됩니다.

- 접근하려는 레지스트리 키.
- 레지스트리 키에 대한 접근 시도를 시작한 프로세스 파일의 전체 이름 및 경로.
- 가능한 응답:
  - **허락** - 위험 처리를 한번 실행합니다.
  - **차단** - 위험 처리를 한번 차단합니다.

이 활동이 컴퓨터에서 시작될 때마다 선택한 처리 작업이 자동으로 수행되도록 하려면 ☑ **규칙 생성** 상자를 체크하십시오.

레지스트리 키에 접근하려고 시도했던 모든 프로그램 활동이 위험하지 않은 경우 해당 프로그램을 신뢰 프로그램 목록에 추가하십시오.

피싱 공격 탐지

카스퍼스키 안티 바이러스에서 피싱 공격을 탐지할 때마다 특별 알림 팝업이 표시됩니다.

이 알림의 내용은 다음과 같습니다.

- 카스퍼스키 랩 바이러스 진단 명에 대한 링크로 제공되는 보안위협의 이름(*피싱 공격*) 및 보안위협에 대한 상세한 개요.
- 피싱 공격에 대한 웹 주소.
- 가능한 응답:
  - **허락** - 피싱 사이트를 계속 다운로드합니다.

- **차단** - 피싱 사이트 다운로드를 차단합니다.

감시 구성요소 또는 작업 동작의 현재 세션에서 탐지된 모든 동일 상태의 개체에 선택한 처리 방법을 적용하려면 ☑ **모두 적용** 상자를 체크하십시오. 현재 세션은 구성요소가 시작된 후부터 중지되거나 프로그램이 다시 시작될 때까지의 시간 또는 바이러스 검사가 시작된 후부터 완료될 때까지의 시간입니다.

감염의심 링크 탐지

의심스러운 웹 주소 목록에 포함되어 있는 주소의 웹사이트를 열면 카스퍼스키 안티 바이러스에서 특별한 알림이 표시합니다.

이 알림의 내용은 다음과 같습니다.

- 웹사이트 주소.
- 가능한 응답:
  - **허락** – 웹사이트 다운로드 진행.
  - **차단** – 웹사이트 다운로드 차단.

감시 구성요소 또는 작업 동작의 현재 세션에서 탐지된 모든 동일 상태의 개체에 선택한 처리 방법을 적용하려면 ☑ **모두 적용** 상자를 체크하십시오. 현재 세션은 구성요소가 시작된 후부터 중지되거나 프로그램이 다시 시작될 때까지의 시간 또는 바이러스 검사가 시작된 후부터 완료될 때까지의 시간입니다.

잘못된 인증서 탐지

SSL 프로토콜을 통한 연결에 대한 보안 확인은 설치된 인증서를 사용하여 수행합니다. 서버에 대한 연결을 시도할 때 잘못된 인증서가 탐지되는 경우(예: 인증서가 침입자에 의해 교체된 경우) 화면에 알림이 표시됩니다.

알림에는 가능한 오류 원인에 대한 정보가 포함되고 원격 포트 및 주소를 확인합니다. 잘못된 인증서에 대한 연결이 계속되는 경우 다음 중 하나를 결정해야 합니다.

- **인증서 수락** - 웹사이트에 대한 연결을 계속합니다.
- **인증서 거부** - 웹사이트에 대한 연결을 중단합니다.
- **인증서 보기** - 인증서에 대한 정보를 확인합니다.

카스퍼스키 안티 바이러스 설정 확인

카스퍼스키 안티 바이러스가 설치 및 구성된 후에 테스트 "바이러스" 및 그 변종을 사용하여 프로그램이 제대로 구성되었는지 확인할 수 있습니다. 각 감시 구성요소/프로토콜별로 별도의 테스트가 필요합니다.

참조:

테스트 "바이러스" EICAR 및 변종 156

HTTP 트래픽 감시 테스트 158

SMTP 트래픽 감시 테스트 158

파일 안티 바이러스 설정 확인 159

바이러스 검사 작업 설정 확인 159

테스트 "바이러스" EICAR 및 변종

이 테스트 "바이러스"는 안티 바이러스 제품의 테스트를 위해 eicar (European Institute for Computer Antivirus Research)에서 특별히 개발한 것입니다.

테스트 "바이러스"에는 컴퓨터에 해를 가할 수 있는 코드가 포함되어 있지 않으므로 바이러스가 아닙니다. 그러나 대부분의 안티 바이러스 제품은 이 파일을 바이러스로 식별합니다.

안티 바이러스 제품의 작동을 테스트하기 위해 실제 바이러스를 사용하지 마십시오.

이 테스트 "바이러스"는 **EICAR** 공식 웹사이트(http://www.eicar.org/anti_virus_test_file.htm)에서 다운로드할 수 있습니다.

파일을 다운로드하기 전에 컴퓨터의 안티 바이러스 감시를 해제해야 합니다. 그렇지 않으면 프로그램에서 *anti_virus_test_file.htm* 파일을 HTTP 프로토콜을 통해 전송된 감염 개체로 식별하여 처리합니다. 테스트 "바이러스"를 다운로드한 후 바로 안티 바이러스 감시를 다시 설정하십시오.

프로그램은 **EICAR** 사이트에서 다운로드한 파일을 **치료할 수 없는** 바이러스가 포함된 감염 개체로 식별하여 이러한 유형의 개체에 지정된 처리 방법을 수행합니다.

또한 표준 테스트 "바이러스"를 변형하여 프로그램 동작을 확인할 수도 있습니다. "바이러스"를 변형하려면 접두사 중 하나를 추가하여(아래 표 참조) 표준 "바이러스"의 내용을 변경하십시오. 테스트 "바이러스"는 하이퍼텍스트 편집기(예: **Microsoft 메모장**, **UltraEdit32** 등)를 사용하여 변형할 수 있습니다.

안티 바이러스 데이터베이스의 최종 업데이트 날짜가 2003년 10월 24일 또는 이후(2003년 10월 누적 업데이트)인 경우에만 변형된 EICAR "바이러스"를 사용하여 안티 바이러스 프로그램의 동작을 정확하게 테스트할 수 있습니다.

아래 표에서 첫 번째 열에는 표준 테스트 "바이러스" 문자열의 처음에 추가해야 하는 접두사가 포함되어 있습니다. 두 번째 열에는 안티 바이러스 프로그램에서 검사 결과를 토대로 개체에 할당할 수 있는 가능한 모든 상태가 나열됩니다. 세 번째 열에는 프로그램에서 지정된 상태의 개체를 처리하는 방법이 나와 있습니다. 개체에서 수행된 실제 처리 작업은 프로그램 설정에 의해 결정됩니다.

테스트 "바이러스"에 접두사를 추가한 후 새 파일을 다른 이름으로 저장하십시오(예: *eicar_dele.com*). 변형된 모든 "바이러스"에 유사한 이름을 할당하십시오.

테스트 "바이러스" 변형

접두사	개체 상태	개체 처리 정보
접두사 없음, 표준 테스트 "바이러스".	**감염됨** 알려진 바이러스 코드를 포함하는 개체입니다. 개체를 치료할 수 없습니다.	프로그램은 개체를 치료할 수 없는 바이러스로 식별합니다. 개체를 치료하려고 시도하는 동안 오류가 발생했습니다. 수행된 처리 방법은 치료할 수 없는 개체에 지정된 방법입니다.
CORR	**손상됨**.	프로그램은 개체에 접근할 수 있지만 손상되었기 때문에 검사할 수 없습니다(예: 파일 구조가 손상되거나 파일 형식이 잘못된 경우). 프로그램 동작에 관한 리포트에서 개체 처리에 대한 정보를 확인할 수 있습니다.
WARN	**감염의심** 알려진 바이러스 코드를 포함하는 개체입니다. 개체를 치료할 수 없습니다.	개체가 휴리스틱 코드 분석기에 의해 감염의심 개체로 확인되었습니다. 탐지 시 안티 바이러스 보안위협 서명 데이터베이스에 이 개체의 치료 절차에 대한 설명이 없습니다. 이러한 유형의 개체가 탐지되면 사용자에게 알립니다.
SUSP?	**감염의심** 알려진 바이러스의 변형된 코드를 포함하는 개체입니다. 개체를 치료할 수 없습니다.	프로그램은 개체 코드의 한 부분이 알려진 바이러스 코드의 한 부분과 일치하는 것을 탐지했습니다. 탐지 시 안티 바이러스 보안위협 서명 데이터베이스에 이 개체의 치료 절차에 대한 설명이 없습니다. 이러한 유형의 개체가 탐지되면 사용자에게 알립니다.
ERRO?	**검사 오류**.	개체를 검사하는 동안 오류가 발생했습니다. 개체의 무결성이 침해당했거나(예: 멀티 볼륨 압축 파일) 개체에 연결되지 않았기 때문에(개체가 네트워크 리소스에서 검사된 경우) 프로그램에서는 개체에 접근할 수 없습니다. 프로그램 동작에 관한 리포트에서 개체 처리에 대한 정보를 확인할 수 있습니다.

접두사	개체 상태	개체 처리 정보
CURE?	**감염됨** 알려진 바이러스 코드를 포함하는 개체입니다. 치료할 수 있습니다.	치료할 수 있는 바이러스를 포함하는 개체입니다. 프로그램은 개체를 치료하고 "바이러스" 본문 텍스트는 CURE 단어로 교체됩니다. 이러한 유형의 개체가 탐지되면 사용자에게 알립니다.
DELE?	**감염됨** 알려진 바이러스 코드를 포함하는 개체입니다. 개체를 치료할 수 없습니다.	프로그램은 개체를 치료할 수 없는 바이러스로 식별합니다. 개체를 치료하려고 시도하는 동안 오류가 발생했습니다. 수행된 처리 방법은 치료할 수 없는 개체에 지정된 방법입니다. 이러한 유형의 개체가 탐지되면 사용자에게 알립니다.

HTTP 트래픽 감시 테스트

- *HTTP 프로토콜을 통해 전송된 데이터 스트림에서 바이러스가 제대로 감지되었는지 확인하려면 다음을 수행하십시오.*

  EICAR 의 공식 웹사이트(http://www.eicar.org/anti_virus_test_file.htm)에서 이 "바이러스" 테스트를 다운로드합니다.

컴퓨터에서 "바이러스" 테스트를 다운로드하려고 하면 카스퍼스키 안티 바이러스가 개체를 감지하여 치료할 수 없는 오염된 개체임을 확인한 다음 해당 상태의 개체에 대해 HTTP 트래픽 검사 설정에서 지정한 작업을 수행합니다. 기본적으로 "바이러스" 테스트를 다운로드하려고 하면 웹사이트와의 연결이 종료되고 브라우저에는 EICAR-Test-File 바이러스에 감염되었다는 메시지가 나타납니다.

SMTP 트래픽 감시 테스트

SMTP 프로토콜을 통해 전송된 데이터 스트림에서 바이러스를 탐지하려면 데이터를 전송하기 위해 이 프로토콜을 사용하는 이메일 시스템을 사용해야 합니다.

안티 바이러스에서 메시지 본문 및 첨부파일을 포함하여 보내는 이메일 메시지를 처리하는 방법을 테스트하는 것이 좋습니다. 메시지 본문에서 바이러스 탐지를 테스트하려면 표준 테스트 "바이러스" 또는 변형된 "바이러스"의 텍스트를 메시지 본문에 복사합니다.

- *그렇게 하려면 다음과 같이 하십시오.*

  1. 컴퓨터에 설치되어 있는 클라이언트를 사용하여 **일반 텍스트** 형식의 메시지를 작성합니다.

  2. RTF 또는 HTML 형식으로 작성된 경우 바이러스 테스트가 포함된 메시지는 검사 대상에서 제외됩니다.

3. 표준 또는 변형된 "바이러스" 텍스트를 메시지 시작 부분에 복사하거나 테스트 "바이러스"가 포함된 파일을 메시지에 첨부합니다.

4. 메시지를 관리자에게 보냅니다.

프로그램에서 개체를 탐지하고 감염된 것으로 식별하여 메시지를 차단합니다.

파일 안티 바이러스 설정 확인

- *파일 안티 바이러스 구성이 정확한지 확인하려면 다음을 수행하십시오.*

    1. 디스크에 폴더를 하나 만듭니다. 공식 **EICAR** 웹사이트(http://www.eicar.org/anti_virus_test_file.htm)에서 다운로드한 "바이러스" 테스트와 사용자가 만든 변종 테스트를 모두 이 폴더로 복사합니다.

    2. 모든 이벤트가 기록되도록 설정하여 보고서 파일에 손상된 개체 또는 오류로 인해 건너뛴 개체가 포함되도록 합니다.

    3. "바이러스" 테스트 또는 변종 버전 중 하나를 실행합니다.

파일 안티 바이러스가 요청을 가로챈 다음 파일을 실행하고 검사하여 해당 상태의 개체에 대해 설정에 지정된 작업을 수행합니다. 감지된 개체별로 수행할 작업을 선택하여 구성요소의 작업에 대해 전체 검사를 수행할 수 있습니다.

파일 안티 바이러스 작업의 결과는 구성요소의 작업에 대한 보고서에서 확인할 수 있습니다.

바이러스 검사 작업 설정 확인

- *바이러스 검사 작업이 제대로 구성되었는지 확인하려면 다음을 수행하십시오.*

    1. 디스크에 폴더를 하나 만듭니다. 공식 **EICAR** 웹사이트(http://www.eicar.org/anti_virus_test_file.htm)에서 다운로드한 "바이러스" 테스트와 사용자가 만든 변종 테스트를 모두 이 폴더로 복사합니다.

    2. 새 바이러스 검사 작업을 만들고 "바이러스" 테스트 집합을 포함하는 폴더를 검사할 개체로 선택합니다.

    3. 모든 이벤트가 기록되도록 설정하여 보고서 파일에 손상된 개체 또는 오류로 인해 검사되지 않은 개체가 포함되도록 합니다.

    4. 바이러스 검사 작업을 실행합니다.

검사 작업이 실행되면 작업 설정에 지정된 작업이 의심스러운 행동을 하거나 감염된 개체가 발견됩니다. 감지된 개체별로 수행할 작업을 선택하여 구성요소의 작업에 대해 전체 검사를 수행할 수 있습니다.

바이러스 검사 작업의 모든 정보는 구성요소의 작업에 대한 보고서에서 확인할 수 있습니다.

명령줄을 통한 프로그램 작업

명령줄에서 카스퍼스키 안티 바이러스 작업을 수행할 수 있습니다. 다음과 같은 작업을 수행할 수 있는 기능이 제공됩니다.

- 프로그램 구성요소 시작 및 중지
- 바이러스 검사 시작 및 중지
- 구성요소와 작업의 현재 상태에 대한 정보 및 통계 표시
- 선택한 개체 검사
- 데이터베이스 및 프로그램 모듈 업데이트
- 명령 프롬프트 구문에서 도움말 불러오기
- 명령 구문에서 도움말 불러오기

명령 프롬프트 구문:

avp.com <명령> [options]

프로그램 설치 폴더 또는 avp.com의 전체 경로를 지정하여 명령줄에서 카스퍼스키 안티 바이러스에 접근해야 합니다.

다음 명령이 제공됩니다.

ACTIVATE	활성화코드를 사용하여 인터넷을 통해 카스퍼스키 안티 바이러스를 활성화합니다.
ADDKEY	라이센스 키 파일을 사용하여 프로그램을 활성화합니다. 카스퍼스키 안티 바이러스 인터페이스를 통해 할당된 암호를 입력한 경우에만 명령을 실행할 수 있습니다.
START	구성요소 또는 작업을 시작합니다.
STOP	구성요소 또는 작업을 중지합니다. 카스퍼스키 안티 바이러스 인터페이스를 통해 할당된 암호를 입력한 경우에만 명령을 실행할 수 있습니다.
STATUS	현재 구성요소 또는 작업 상태를 화면에 표시합니다.
STATISTICS	구성요소 또는 작업에 대한 통계를 화면에 표시합니다.

HELP	명령 구문 및 명령 목록에 대한 도움말을 제공합니다.
SCAN	개체에서 바이러스를 검사합니다.
UPDATE	프로그램 업데이트를 시작합니다.
ROLLBACK	마지막 카스퍼스키 안티 바이러스 업데이트로 롤백합니다. 카스퍼스키 안티 바이러스 인터페이스를 통해 할당된 암호를 입력한 경우에만 명령을 실행할 수 있습니다.
EXIT	프로그램을 닫습니다. 카스퍼스키 안티 바이러스 인터페이스를 통해 할당된 암호를 입력한 경우에만 명령을 실행할 수 있습니다.
IMPORT	프로그램 감시 설정을 가져옵니다. 카스퍼스키 안티 바이러스 인터페이스를 통해 할당된 암호를 입력한 경우에만 명령을 실행할 수 있습니다.
EXPORT	프로그램 감시 설정을 내보냅니다.

각 명령에는 고유한 파라미터 집합이 필요합니다.

참조:

프로그램 활성화 162

프로그램 구성요소 및 작업 관리 162

바이러스 검사 164

프로그램 업데이트 168

마지막으로 성공한 업데이트로 롤백 169

감시 설정 내보내기 169

감시 설정 가져오기 170

프로그램 시작 170

프로그램 중지 170

추적 파일 생성 170

도움말 보기 171

명령줄 코드 반환 171

프로그램 활성화

카스퍼스키 안티 바이러스를 활성화하는 데는 다음 두 가지 방법을 사용할 수 있습니다.

- 인터넷을 통해 활성화 코드 사용(ACTIVATE 명령)
- 라이센스 키 파일 사용(ADDKEY 명령)

명령 구문:

ACTIVATE <활성화_코드>

ADDKEY <파일_이름> /password=<사용자_암호>

설정 내용:

<활성화_코드>	라이센스 구입 시 제공된 프로그램 활성화코드
<파일_이름>	*.key 확장자를 갖는 프로그램 라이센스 키 파일 이름
<사용자_암호>	인터페이스에서 지정된 프로그램 암호

ADDKEY 명령은 암호를 입력하지 않으면 실행되지 않습니다.

예:

avp.com ACTIVATE 11AA1-11AAA-1AA11-1A111

avp.com ADDKEY 1AA111A1.key /password=<사용자_암호>

프로그램 구성요소 및 작업 관리

명령 구문:

avp.com <명령> <프로필|작업_이름> [/R[A]:<리포트_파일>]

avp.com STOP|PAUSE <프로필|작업_이름> /password=<사용자_암호> [/R[A]:<리포트_파일>]

<명령>	명령 프롬프트에서 다음 명령을 사용하여 카스퍼스키 안티 바이러스 구성요소 및 작업을 관리할 수 있습니다. START – 실시간 감시 구성요소 또는 작업을 시작합니다. STOP – 실시간 감시 구성요소 또는 작업을 중지합니다. (STOP 명령은 암호 없이 수락되지 않습니다.) STATUS – 실시간 감시 구성요소 또는 작업의 현재 상태를 표시합니다. STATISTICS – 실시간 감시 구성요소 또는 작업에 대한 통계를 화면에

	출력합니다.
<프로필|작업_이름>	카스퍼스키 안티 바이러스의 실시간 감시 구성요소, 구성요소 모듈, 필요 시 검사 또는 업데이트 작업을 **<프로필>** 설정 값으로 지정할 수 있습니다(카스퍼스키 안티 바이러스에서 사용하는 표준 값은 아래 표와 같습니다). 필요 시 검사 또는 업데이트 작업 이름을 **<작업_이름>** 설정 값으로 지정할 수 있습니다.
<사용자_암호>	인터페이스에서 지정된 프로그램 암호입니다.
/R[A]:<리포트_파일>	**/R:<리포트_파일>** – 중요한 이벤트만 리포트에 기록합니다. **/RA:<리포트_파일>** – 모든 이벤트를 리포트에 기록합니다. 파일에 대한 절대 경로 또는 상대 경로를 사용할 수 있습니다. 파라미터가 정의되지 않은 경우 화면에 결과가 표시되고 모든 이벤트가 나타납니다.

<프로필> 설정은 다음 값 중 하나를 가질 수 있습니다.

RTP	모든 실시간 감시 구성요소입니다. 실시간 감시가 완전히 중지되어 있는 경우 **avp.com START RTP** 명령을 사용하면 모든 실시간 감시 구성요소가 실행됩니다. 명령 프롬프트에서 **STOP** 명령을 사용하여 구성요소를 중지한 경우 **avp.com START RTP** 명령을 사용하여 실행할 수 없습니다. 구성요소를 시작하려면 **<프로필>**에 특정 실시간 감시 구성요소의 이름을 입력하고 **avp.com START <프로필>** 명령을 실행해야 합니다. 예를 들면 **avp.com START FM** 을 실행합니다.
pdm	사전 방역
FM	파일 안티 바이러스
EM	메일 안티 바이러스

WM	웹 안티 바이러스 웹 안티 바이러스 하위 구성요소 값: **httpscan (HTTP)** – HTTP 트래픽 검사 **sc** – 스크립트 검사
IM	메신저 안티 바이러스
Updater	업데이트
Rollback	마지막으로 성공한 업데이트로 롤백
Scan_My_Computer	컴퓨터 검사
Scan_Objects	개체 검사
Scan_Quarantine	격리저장소 검사
Scan_Rootkits	루트킷 검사
Scan_Startup (STARTUP)	시작 개체 검사
Scan_Vulnerabilities (SECURITY)	취약점 검사

명령 프롬프트에서 시작되는 구성요소 및 작업은 프로그램 인터페이스에 구성된 설정으로 실행됩니다.

예:

- *파일 안티 바이러스 구성요소 유형을 작동하려면 명령 프롬프트에 다음을 입력합니다.*

  avp.com START FM

- *유해 사이트 차단을 다시 시작하려면 명령 프롬프트에 다음을 입력합니다.*

  avp.com RESUME ParCtl

- *명령 프롬프트에서 컴퓨터 검사 작업을 중지하려면 다음을 입력합니다.*

  avp.com STOP Scan_My_Computer /password=<your_password>

바이러스 검사

명령 프롬프트를 사용하여 특정 영역에서 바이러스 검사를 시작하고 악성 개체를 처리하는 구문은 일반적으로 다음과 같습니다.

avp.com SCAN [<검사한_개체>] [<처리_방법>] [<파일_형태>] [<제외>] [<구성_파일>] [<리포트_설정>]

[<고급_설정>]

개체를 검사하기 위해 명령줄에서 필요한 작업을 시작하여 프로그램에서 생성된 작업을 사용할 수도 있습니다. 작업은 카스퍼스키 안티 바이러스 인터페이스에서 지정된 설정을 사용하여 실행됩니다.

설정 내용:

<검사할_개체> – 이 파라미터는 악성 코드를 검사할 개체 목록을 제공합니다. 이 파라미터는 제공된 목록에 있는 몇 개의 값을 공백으로 구분하여 포함할 수 있습니다.	
<파일>	검사할 파일 및/또는 폴더 경로 목록입니다. 파일에 대한 절대 경로 또는 상대 경로를 입력할 수 있습니다. 목록에 있는 항목은 공백으로 구분됩니다. 설명: • 개체 이름에 공백이 포함된 경우 따옴표를 사용해야 합니다. • 특정 폴더를 참조하는 경우 해당 폴더에 있는 모든 파일이 검사됩니다.
/MEMORY	RAM 개체
/STARTUP	자동 시작 개체
/MAIL	사서함
/REMDRIVES	모든 이동식 장치 드라이브
/FIXDRIVERS	모든 내부 드라이브
/NETDRIVES	모든 네트워크 드라이브
/QUARANTINE	격리된 개체
/ALL	전체 컴퓨터 검사
/@:<파일_목록>	검사할 개체 및 카탈로그 목록이 포함된 파일 경로입니다. 파일은 텍스트 형식이어야 하며 각 검사 개체를 별도의 줄에 나열해야 합니다. 파일에 대한 절대 경로 또는 상대 경로를 입력할 수 있습니다. 경로에 공백이 포함된 경우 따옴표를 사용해야 합니다.
<처리_방법> – 이 파라미터는 검사 중에 탐지된 악성 개체에 대해 수행할 처리 방법을 결정합니다. 이 파라미터가 정의되지 않은 경우 기본 처리 방법은 **/i8** 값을 갖는 처리 방법입니다.	

/i0	개체에 대해 처리 방법을 수행하지 않고 리포트에 정보를 기록하기만 합니다.
/i1	감염 개체를 처리하고 치료가 불가능한 경우 건너뜁니다.
/i2	감염 개체를 처리하고 치료에 실패한 경우 삭제합니다. 복합 개체에서 감염된 개체를 삭제하지 않습니다. 감염된 복합 개체는 실행 가능한 헤더(sfx 압축 파일)를 사용하여 삭제합니다(기본 설정).
/i3	감염 개체를 처리하고 치료에 실패한 경우 삭제합니다. 감염된 부분을 삭제할 수 없는 경우 모든 복합 개체를 완전히 삭제합니다.
/i4	감염 개체를 삭제합니다. 감염된 부분을 삭제할 수 없는 경우 모든 복합 개체를 완전히 삭제합니다.
/i8	감염 개체가 탐지될 경우 사용자에게 처리 방법을 묻는 메시지를 표시합니다.
/i9	검사가 끝나면 사용자에게 처리 방법을 묻는 메시지를 표시합니다.
<파일_형태> – 이 파라미터는 안티 바이러스 검사를 받을 파일 형식을 정의합니다. 이 파라미터가 정의되지 않은 경우 기본적으로 감염된 파일만 컨텐츠별로 검사됩니다.	
/fe	감염된 파일만 확장자별로 검사합니다.
/fi	감염된 파일만 컨텐츠별로 검사합니다.
/fa	모든 파일을 검사합니다.
<제외> – 이 파라미터는 검사에서 제외되는 개체를 정의합니다. 이 파라미터는 제공된 목록에 있는 몇 개의 값을 공백으로 구분하여 포함할 수 있습니다.	
-e:a	압축 파일을 검사하지 않습니다.
-e:b	이메일 데이터베이스를 검사하지 않습니다.
-e:m	일반 텍스트 이메일을 검사하지 않습니다.
-e:<파일_마스크>	마스크와 일치하는 개체를 검사하지 않습니다.
-e:<초>	**<초>** 파라미터에 지정한 시간 이상 검사된 개체는 건너뜁니다.
-es:<크기>	크기(MB)가 **<크기>** 파라미터에 지정된 값을 초과하는 개체는 건너뜁니다.

<구성_파일> – 검사에 대한 프로그램 설정이 포함된 구성 파일 경로를 정의합니다. 구성 파일은 일반 텍스트 형식이고 안티 바이러스 검사에 대한 명령줄 파라미터 집합을 포함합니다. 파일에 대한 절대 경로 또는 상대 경로를 입력할 수 있습니다. 이 파라미터를 지정하지 않은 경우 프로그램 인터페이스에 설정된 값이 사용됩니다.	
/C:<파일_이름>	**<파일_이름>** 구성 파일에 지정된 설정 값을 사용합니다.
<리포트_설정> – 이 파라미터는 검사 결과에 대한 리포트 형식을 결정합니다. 파일에 대한 절대 경로 또는 상대 경로를 사용할 수 있습니다. 파라미터가 정의되지 않은 경우 화면에 결과가 표시되고 모든 이벤트가 나타납니다.	
/R:<리포트_파일>	중요한 이벤트만 이 파일에 기록합니다.
/RA:<리포트_파일>	모든 이벤트를 이 파일에 기록합니다.
<advanced settings> – settings that define the use of anti-virus scanning technologies.	
/iChecker=<on|off>	iChecker 기술 사용을 작동/중지합니다.
/iSwift=<on|off>	iSwift 기술 사용을 작동/중지합니다.

예:

- *메모리, 자동 시작 프로그램, 사서함, My Documents 및 Program Files 디렉터리와 test.exe 파일 검사를 시작합니다.*

  avp.com SCAN /MEMORY /STARTUP /MAIL "C:₩Documents and Settings₩All Users₩My Documents" "C:₩Program Files" "C:₩Downloads₩test.exe"

- *선택한 개체 검사를 일시 중지하고 전체 컴퓨터 검사를 시작한 후 일시 중지한 검사를 계속합니다.*

  avp.com PAUSE Scan_Objects /password=<사용자_암호>

  avp.com START Scan_My_Computer

  avp.com RESUME Scan_Objects

- *작업 구성 파일 scan_setting.txt 를 사용하여 object2scan.txt 파일에 나열된 개체를 검사합니다. scan_setting.txt 구성 파일을 사용합니다. 검사가 완료되면 모든 이벤트를 기록하는 리포트를 생성합니다.*

  avp.com SCAN /MEMORY /@:objects2scan.txt /C:scan_settings.txt /RA:scan.log

구성 파일 예제:

/MEMORY /@:objects2scan.txt /C:scan_settings.txt /RA:scan.log

프로그램 업데이트

명령줄에서 카스퍼스키 안티 바이러스 모듈 및 프로그램 데이터베이스를 업데이트하기 위한 구문은 다음과 같습니다.

avp.com UPDATE [<업데이트_경로>] [/R[A]:<리포트_파일>] [/C:<파일_이름>] [/APP=<on|off>]

설정 내용:

<업데이트_경로>	업데이트를 다운로드하기 위한 HTTP/FTP 서버 또는 네트워크 폴더입니다. 파라미터 값은 업데이트 전체 경로 또는 URL 이 될 수 있습니다. 경로를 선택하지 않으면 프로그램 업데이트 설정에 지정된 업데이트 경로가 사용됩니다.
/R[A]:<리포트_파일>	**/R:<리포트_파일>** – 중요한 이벤트만 리포트에 기록합니다. **/RA:<리포트_파일>** – 모든 이벤트를 리포트에 기록합니다. 파일에 대한 절대 경로 또는 상대 경로를 사용할 수 있습니다. 파라미터가 정의되지 않은 경우 화면에 결과가 표시되고 모든 이벤트가 나타납니다.
/C:<파일_이름>	카스퍼스키 안티 바이러스 업데이트 설정이 포함된 구성 경로입니다. 구성 파일은 프로그램 업데이트에 대한 명령줄 파라미터 목록이 포함된 일반 텍스트 형식 파일입니다. 파일에 대한 절대 경로 또는 상대 경로를 입력할 수 있습니다. 이 파라미터를 지정하지 않은 경우 프로그램 인터페이스 설정에 지정된 값이 사용됩니다.
/APP=<on|off>	프로그램 모듈 업데이트를 작동/중지합니다.

예:

- *프로그램 데이터베이스를 업데이트하고 모든 이벤트를 리포트에 기록:*

  avp.com UPDATE /RA:avbases_upd.txt

- *updateapp.ini 구성 파일의 파라미터를 사용하여 카스퍼스키 안티 바이러스 프로그램 업데이트:*

  avp.com UPDATE /APP=on /C:updateapp.ini

구성 파일 예제:

"ftp://my_server/kav updates" /RA:avbases_upd.txt /app=on

마지막으로 성공한 업데이트로 롤백

명령 구문:

ROLLBACK [/R[A]:<리포트_파일>] [/password=<사용자_암호>]

설정 내용:

/R[A]:<리포트_파일>	**/R:**<리포트_파일> – 중요한 이벤트만 리포트에 기록합니다. **/RA:**<리포트_파일> – 모든 이벤트를 리포트에 기록합니다. 파일에 대한 절대 경로 또는 상대 경로를 사용할 수 있습니다. 파라미터가 정의되지 않은 경우 화면에 결과가 표시되고 모든 이벤트가 나타납니다.
<사용자_암호>	인터페이스에서 지정된 프로그램 암호

이 명령은 암호 없이 수락되지 않습니다.

예:

avp.com ROLLBACK /RA:rollback.txt /password=<사용자_암호>

감시 설정 내보내기

명령 구문:

avp.com EXPORT <프로필> <파일_이름>

설정 내용:

<프로필>	내보내는 설정이 포함된 구성요소 또는 작업입니다. **<프로필>** 설정에는 "프로그램 구성요소 및 작업 관리" 도움말 섹션에 나열된 모든 값을 사용할 수 있습니다.
<파일_이름>	카스퍼스키 안티 바이러스 설정을 내보내는 파일의 경로입니다. 절대 경로 또는 상대 경로를 지정할 수 있습니다. 다른 형식이 지정되지 않거나 형식이 아예 지정되지 않은 경우 구성 파일은 이진 형식(*DAT*)으로 저장됩니다. 구성 파일은 이후에 프로그램 설정을 다른 컴퓨터에 내보내는 데 사용될 수 있습니다. 또한 파일 이름에 *.txt* 확장자를 입력하여 텍스트 파일로도 저장할 수 있습니다. 텍스트 파일에서는 감시 설정을 가져올 수 없으며, 카스퍼스키 안티 바이러스 작업에 대한 메인 설정을 지정하는 데만 사용할 수 있습니다.

예:

avp.com EXPORT c:₩settings.dat

감시 설정 가져오기

명령 구문:

avp.com IMPORT <파일_이름>[/password=<사용자_암호>]

<파일_이름>	카스퍼스키 안티 바이러스 설정을 가져오는 파일의 경로입니다. 절대 경로 또는 상대 경로를 지정할 수 있습니다.
<사용자_암호>	프로그램 인터페이스에 지정된 카스퍼스키 안티 바이러스 암호입니다. 암호는 이진 파일에서만 가져올 수 있습니다.

이 명령은 암호 없이 수락되지 않습니다.

예:

avp.com IMPORT c:₩settings.dat /password=<사용자_암호>

프로그램 시작

명령 구문:

avp.com

프로그램 중지

명령 구문:

EXIT /password=<사용자_암호>

<사용자_암호>	인터페이스에서 지정된 프로그램 암호

이 명령은 암호 없이 수락되지 않습니다.

추적 파일 생성

카스퍼스키 안티 바이러스에 문제가 있는 경우 추적 파일을 생성할 수 있습니다. 추적 파일은 문제 해결에 유용하게 쓰이기 때문에 기술 지원 전문가들이 널리 사용합니다.

명령 구문:

avp.com TRACE [file] [on|off] [<추적_레벨>]

설정 내용:

[on|off]	추적 파일 생성 작동/중지
[file]	파일에 추적 출력
<추적_레벨>	이 값은 0(최소 레벨, 중요 메시지만)에서 700(최대 레벨, 모든 메시지)까지의 정수가 될 수 있습니다. 기술 지원 서비스에 문의하면 필요한 추적 레벨을 알려줄 것입니다. 지정되지 않은 경우 이 값을 500 으로 설정할 것을 권장합니다.

특정 문제를 해결하기 위해서만 추적 파일을 생성하는 것이 좋습니다. 정기적으로 추적을 작동하면 컴퓨터 속도가 느려지고 하드 드라이브 공간이 소모될 수 있습니다.

예:

- *추적 파일 생성 중지:*

  avp.com TRACE file off

- *기술 지원 서비스에 전송하도록 최대 추적 레벨 500 을 사용하여 추적 파일 생성:*

  avp.com TRACE file on 500

도움말 보기

프로그램 명령줄 구문을 보려면 다음 명령을 사용합니다.

avp.com [/? | HELP]

다음 명령 중 하나를 사용하여 특정 명령 구문에 대한 도움말을 확인할 수 있습니다.

avp.com <명령> /?

avp.com HELP <명령>

명령줄 반환 코드

이 섹션에는 명령줄에서 반환되는 코드 목록이 포함되어 있습니다. 작업에 관계없이 명령줄에서 명령 사용 시 반환되는 일반 코드와 특정 종류의 작업에서만 반환되는 코드로 구분할 수 있습니다.

일반 반환 코드	
0	작업을 성공적으로 완료

1	잘못된 설정 값
2	알 수 없는 오류
3	작업 완료 오류
4	작업 취소됨
바이러스 검사 작업 반환 코드	
101	모든 위험 개체가 처리됨
102	위험 개체가 탐지됨

문제 제거

카스퍼스키 안티 바이러스 작업 중에 문제가 발생할 경우 먼저 해결 방법이 프로그램 도움말 시스템 또는 카스퍼스키 랩 자주 묻는 질문에 있는지 확인합니다. *자주 묻는 질문*은 기술 지원 웹사이트의 별도 섹션으로서 카스퍼스키 랩 제품에 대한 권장 사항 및 자주 묻는 질문에 대한 답변으로 이루어져 있습니다. 이 리소스를 통해 질문에 대한 답변 또는 문제 해결 방법을 찾아보십시오.

- *자주 묻는 질문의 사용은 다음과 같습니다:*

  1. 메인 프로그램 창을 엽니다.
  2. 창 하단에서 **지원** 링크를 누릅니다.
  3. 열리는 **지원** 창에서 **자주 묻는 질문** 링크를 누릅니다.

카스퍼스키 안티 바이러스 작업에 대한 정보를 얻을 수 있는 또 다른 리소스는 카스퍼스키 랩 고객 포럼입니다. 기술 지원 웹사이트의 또 다른 별도 섹션으로 사용자 질문, 정보 제공 및 요청사항이 포함되어 있습니다. 포럼의 주요 주제를 살펴보고, 의견을 남기거나 질문에 대한 답변을 찾을 수 있습니다.

- *고객 포럼에 방문하는 방법은 다음과 같습니다:*

  1. 메인 프로그램 창을 엽니다.
  2. 창 하단에서 **지원** 링크를 누릅니다.
  3. 열리는 **지원** 창에서 **고객 포럼** 링크를 누릅니다.

프로그램 도움말 시스템, 자주 묻는 질문 또는 고객 포럼에서 문제에 대한 해결 방법을 찾을 수 없는 경우 카스퍼스키 랩 기술 지원 서비스에 문의하십시오.

참조:

시스템 상태 리포트 생성 173

추적 파일 생성 174

데이터 파일 전송 175

AVZ 스크립트 실행 176

시스템 상태 리포트 생성

카스퍼스키 랩 전문가는 사용자의 문제를 해결할 때 시스템 상태에 대한 리포트를 요청할 수 있습니다. 이 리포트에는 실행되는 프로세스, 로드된 모듈 및 드라이버, Microsoft Internet Explorer 및 Microsoft Windows Explorer 플러그인, 열린 포트, 탐지된 감염의심 개체 등에 대한 자세한 정보가 포함되어 있습니다.

시스템 상태 리포트가 생성될 때 사용자의 개인 정보는 수집되지 않습니다.

- *시스템 상태 리포트를 생성하는 방법은 다음과 같습니다:*

  1. 메인 프로그램 창을 엽니다.
  2. 창 하단에서 **지원** 링크를 누릅니다.
  3. 열리는 **지원** 창에서 **지원 도구** 링크를 누릅니다.
  4. 열리는 **기술 지원 서비스에 필요한 정보** 창에서 **시스템 상태 리포트 만들기** 버튼을 누릅니다.

- *시스템 상태 리포트는 HTML 및 XML 형식으로 생성되어 sysinfo.zip 압축 파일로 저장됩니다. 정보 수집 프로세스가 완료되면 리포트를 볼 수 있습니다.*

- *리포트를 보는 방법은 다음과 같습니다:*

  1. 메인 프로그램 창을 엽니다.
  2. 창 하단에서 **지원** 링크를 누릅니다.
  3. 열리는 **지원** 창에서 **지원 도구** 링크를 누릅니다.
  4. 열리는 **기술 지원 서비스에 필요한 정보** 창에서 **보기** 버튼을 누릅니다.
  5. *sysinfo.zip* 압축 파일을 엽니다. 여기에 리포트 파일이 포함되어 있습니다.

추적 파일 생성

- 카스퍼스키 안티 바이러스를 설치하고 나면 운영 체제 또는 개별 프로그램 작동에 약간의 오류가 발생할 수 있습니다. 그 원인은 대부분 카스퍼스키 안티 바이러스와 컴퓨터에 설치된 소프트웨어 또는 컴퓨터 구성요소 드라이버가 충돌하기 때문입니다. 카스퍼스키 전문가는 사용자의 문제를 성공적으로 해결하기 위해 추적 파일을 생성하도록 요청할 수 있습니다.

- *추적 파일을 생성하는 방법은 다음과 같습니다:*

  1. 메인 프로그램 창을 엽니다.
  2. 창 하단에서 **지원** 링크를 누릅니다.
  3. 열리는 **지원** 창에서 **지원 도구** 링크를 누릅니다.
  4. 열리는 **기술 지원 서비스에 필요한 정보** 창에서 **추적로그** 섹션의 드롭다운 목록을 사용하여 추적 레벨을 선택합니다. 추적 레벨은 기술 지원 전문가가 권장하는 대로 설정해야 합니다. 기술 지원 전문가가 추적 레벨을 권장하지 않는 경우 **500** 으로 설정하는 것이 좋습니다.
  5. 추적 프로세스를 시작하려면 **작동** 버튼을 누릅니다.

6. 문제가 발생하게 된 상황을 재현합니다.

7. 추적 프로세스를 중지하려면 **중지** 버튼을 누릅니다.

카스퍼스키 랩 서버에 추적 결과 업로드로 전환할 수 있습니다.

데이터 파일 전송

추적 파일 및 시스템 상태 리포트를 생성한 후 카스퍼스키 랩 지원 전문가에게 전송해야 합니다.

기술 지원 서버에 데이터 파일을 업로드하려면 요청사항 번호가 필요합니다. 요청사항 번호는 요청이 활성화된 경우 기술 지원 웹사이트 Personal Cabinet에 표시됩니다.

- *지원 서비스 서버에 데이터 파일을 업로드하는 방법은 다음과 같습니다:*

  1. 메인 프로그램 창을 엽니다.

  2. 창 하단에서 **지원** 링크를 누릅니다.

  3. 열리는 **지원** 창에서 **지원 도구** 링크를 누릅니다.

  4. 열리는 **기술 지원 서비스에 필요한 정보** 창의 **처리** 섹션에서 **서버에 기술 지원 서비스 용 정보 전송** 버튼을 누릅니다.

  5. 열리는 창에서 지원 서비스에 전송할 추적 파일 옆에 있는 상자를 체크하고 **전송** 버튼을 누릅니다.

  6. 열리는 **요청사항 번호 입력** 창에서 지원 서비스 사이트에서 전자 양식 작성 시 요청에 할당된 번호를 지정합니다.

선택한 추적 파일은 압축되어 지원 서비스 서버로 전송됩니다.

어떠한 이유로 기술 지원 서비스에 문의할 수 없는 경우 컴퓨터에 데이터 파일을 저장할 수 있습니다.

- *디스크에 데이터 파일을 저장하는 방법은 다음과 같습니다:*

  1. 메인 프로그램 창을 엽니다.

  2. 창 하단에서 **지원** 링크를 누릅니다.

  3. 열리는 **지원** 창에서 **지원 도구** 링크를 누릅니다.

  4. 열리는 **기술 지원 서비스에 필요한 정보** 창의 **처리** 섹션에서 **서버에 기술 지원 서비스 용 정보 전송** 버튼을 누릅니다.

  5. 열리는 창에서 지원 서비스에 전송할 추적 파일 옆에 있는 상자를 체크하고 **전송** 버튼을 누릅니다.

  6. 열리는 **요청사항 번호 입력** 창에서 **취소** 버튼을 누르고 디스크에 파일 저장을 확인합니다.

  7. 열리는 창에서 압축 파일 이름을 지정합니다

이후에 Personal Cabinet을 통해 기술 지원 서비스에 저장한 파일을 전송할 수 있습니다.

AVZ 스크립트 실행

카스퍼스키 랩 전문가는 추적 파일 및 시스템 상태 리포트를 사용하여 문제를 분석합니다. 분석 결과는 탐지된 문제를 제거하기 위한 일련의 처리 방법입니다. 이러한 처리 방법 목록은 상당히 길 수 있습니다.

이러한 절차를 간소화하기 위해 AVZ 스크립트가 사용됩니다. AVZ 스크립트는 레지스트리 키 편집, 파일 격리, 파일 종류 검색 및 관련 파일 격리, UserMode 및 KernelMode 인터셉터 차단을 수행하는 명령 집합입니다.

카스퍼스키 안티 바이러스에는 스크립트를 실행하기 위한 *AVZ 스크립트 실행 마법사*가 포함되어 있습니다. 마법사는 **다음** 및 **뒤로** 버튼을 사용하여 이동하는 일련의 화면(단계)으로 구성됩니다. 작업이 완료된 후 마법사를 닫으려면 **끝내기** 버튼을, 어느 단계에서나 마법사를 중지하려면 **취소** 버튼을 사용하십시오.

카스퍼스키 랩 전문가에게서 받은 AVZ 스크립트의 텍스트를 변경하지 않는 것이 좋습니다. 스크립트 실행 중 문제가 발생하는 경우 기술 지원 서비스에 문의하십시오.

- *마법사를 시작하는 방법은 다음과 같습니다:*

  1. 메인 프로그램 창을 엽니다.
  2. 창 하단에서 **지원** 링크를 누릅니다.
  3. 열리는 **지원** 창에서 하단의 **지원 도구** 링크를 누릅니다.
  4. 열리는 **기술 지원 서비스에 필요한 정보** 창에서 **AVZ 스크립트 실행하기** 버튼을 누릅니다

스크립트가 성공적으로 실행되면 마법사가 닫히고, 스크립트 실행 도중 오류가 발생하면 관련 오류 메시지가 마법사에 표시됩니다.

카스퍼스키 시큐리티 네트워크 데이터 수집 정책

A. 소개

본 문서에는 카스퍼스키 랩의 서비스 또는 소프트웨어를 사용하기 전에 반드시 알아두어야 하는 중요한 정보가 수록되어 있으므로 자세히 읽어 주십시오. 카스퍼스키 랩 소프트웨어 및 서비스를 계속 사용함으로써 사용자는 본 카스퍼스키 랩의 데이터 수집 정책을 동의한 것으로 간주됩니다. 카스퍼스키 랩은 본 페이지에 변경 사항을 게시하는 방법으로 언제든지 본 데이터 수집 정책을 수정할 권한을 보유합니다. 아래 개정 날짜를 확인하여 가장 최근에 검토한 후 본 정책이 수정되었는지 확인해 보십시오. 업데이트된 데이터 수집 정책을 게시한 후에도 카스퍼스키 랩에서 제공하는 서비스를 계속해서 사용하는 것은 변경 사항을 수락하는 것으로 간주됩니다.

카스퍼스키 랩 및 해당 자회사(통칭하여 "카스퍼스키 랩")는 카스퍼스키 안티 바이러스 및 카스퍼스키 안티 바이러스에 대한 데이터 수집 및 유포 절차를 알리고 공개하기 위해 본 데이터 수집 정책을 마련했습니다.

카스퍼스키 랩의 약속

카스퍼스키 랩은 모든 사용자에게 최상의 서비스를 제공하고 특히 데이터 수집에 관한 사용자의 우려를 불식시키기 위한 강한 의지를 가지고 있습니다. 본 정책은 카스퍼스키 시큐리티 네트워크에서 정보 및 데이터를 수집하여 사용하는 방식에 대해 궁금해 하는 많은 사용자를 위해 카스퍼스키 시큐리티 네트워크를 관장하는 데이터 수집 원리("데이터 수집 정책" 또는 "정책")를 알려드리기 위해 마련된 것입니다.

본 데이터 수집 정책에는 사용자의 데이터 수집에 관한 우려 사항을 해결해 드리기 위해 카스퍼스키 랩에서 취하고 있는 몇 가지 단계에 대한 자세한 정보가 기술적인 측면과 함께 수록되어 있습니다. 본 데이터 수집 정책은 주요 프로세스 및 영역별로 구성되어 있어서 사용자는 관련 정보를 빠르게 검토할 수 있습니다 본 정책의 궁극적은 목적은 사용자의 요구 사항과 기대치를 충족함으로써 수집된 데이터의 보호를 비롯한 비즈니스의 기반을 다지기 위한 것입니다.

데이터 및 정보는 카스퍼스키 랩에서 수집합니다. 본 데이터 수집 정책을 검토한 후 데이터 수집과 관련하여 궁금한 사항이 있으시면 이메일(support@kaspersky.co.kr)로 문의하시기 바랍니다.

카스퍼스키 시큐리티 네트워크란 무엇입니까?

카스퍼스키 시큐리티 네트워크 서비스는 전 세계 카스퍼스키 랩 보안 제품 사용자가 자신의 컴퓨터를 대상으로 하는 새로운 보안 위험으로부터 컴퓨터를 보호하는 데 필요한 확인 과정을 간소화하고 시간을 단축할 수 있도록 지원합니다. 새로운 보안위협과 그 출처를 파악하고 사용자 보안 및 제품 기능을 강화하기 위해 카스퍼스키 시큐리티 네트워크는 선택한 보안 및 프로그램 데이터를 수집하여 카스퍼스키 랩에 분석을 의뢰합니다. 해당 정보에는 사용자에 대한 개인 식별 정보는 포함되지 않으며 카스퍼스키 랩에서는 악성 보안위협 및 바이러스를 차단하는 보안 제품 및 솔루션을 향상시키는 것 이외의 다른 목적으로는 해당 정보를 사용하지 않습니다. 실수로 사용자의 개인 데이터가 전송된 경우 카스퍼스키 랩은 본 데이터 수집 정책에 의거하거 해당 데이터를 유지 및 보호해야 합니다.

전 세계 카스퍼스키 랩 보안 제품 사용자는 카스퍼스키 시큐리티 네트워크에 참여함으로써 안전한 인터넷 환경을 만드는 데 기여하게 됩니다.

법률 문제

카스퍼스키 랩에서 제공하는 서비스는 미국을 포함한 여러 관할 지역에서 사용될 수 있으므로 카스퍼스키 시큐리티 네트워크는 해당 관할 지역의 법률을 준수합니다. 카스퍼스키 랩은 법률에서 요구하는 경우 또는 카스퍼스키 랩 게스트, 방문자, 제휴자, 자산 등에 해로운 활동으로부터 보호하거나 이를 조사하기 위해 필요한 경우 사용자의 허락 없이 개인 식별 정보를 공개해야 합니다. 위에서 언급된 대로 카스퍼스키 시큐리티 네트워크에서 수집한 데이터 및 정보와 관련된 법률은 국가마다 다를 수 있습니다. 예를 들어, EU 및 회원국에서 수집한 일부 개인 식별 정보는 전자 통신 부문에서 개인 데이터 처리 및 개인정보보호에 관하여 2002 년 7 월 12 일 제정된 유럽의회 및 유럽이사회의 Directive 2002/58/EC, 개인 데이터의 처리와 관련한 개인 보호 및 해당 데이터의 자유로운 이동에 관하여 1995 년 10 월 24 일 제정된 유럽의회 및 유럽이사회의 Directive 95/46/EC 및 EU 회원국에서 채택한 사후입법, 표준 계약 조항(제 3 국가로 전송된 개인 데이터)에 관한 유럽 위원회 결정 497/2001/EC 및 EU 회원국에서 채택한 사후입법 등 개인 데이터, 개인정보보호, 전자 통신 등에 관한 EU Directives 를 준수합니다.

카스퍼스키 시큐리티 네트워크는 위에서 언급한 정보를 처음으로 수집할 때 비즈니스 개발을 위한 목적으로 한 해당 정보의 공유 사실을 관련 사용자에게 알려야 하여, 해당 데이터의 상업적인 사용 및 제 3 자에게 전송하는 것을 온라인으로 수락(EU 회원국 및 참여 절차를 요구하는 기타 국가) 또는 거부(기타 모든 국가에 대해)할 수 있는 기회를 해당 인터넷 사용자에게 제공해야 합니다.

법률 집행에 의해 또는 사법 당국에서 카스퍼스키 랩에 개인 식별 정보를 해당 정부 기관에 제공하도록 요구할 수 있습니다. 법률 집행 또는 사법 당국에서 요구하는 경우 카스퍼스키 랩은 관련 문서를 받은 즉시 해당 정보를 제공해야 합니다. 또한 카스퍼스키 랩은 법령에서 허용한 대로 당사의 자산 및 개인의 건강과 안전을 보호할 목적으로 법률 집행을 위해 정보를 제공할 수 있습니다.

개인 데이터 보호 회원국 당국에 대한 선언은 EU 회원국의 유효한 사후입법에 의거하여 작성되어야 합니다. 해당 선언에 대한 정보는 카스퍼스키 시큐리티 네트워크 서비스에서 이용할 수 있습니다

.

B. 수집 정보

카스퍼스키 랩에서 수집하는 데이터 카스퍼스키 랩에서 수집하는 데이터

사용자는 본 정책에 따라 데이터를 제공할 권한이 있으며 카스퍼스키 시큐리티 네트워크 서비스는 사용자 컴퓨터의 잠재적인 보안 위험에 대한 핵심 데이터 및 확장 데이터를 수집하여 카스퍼스키 랩에 제출할 수 있습니다. 수집한 데이터는 다음과 같습니다:

- 핵심 데이터
    - 설치되어 있는 운영 체제 및 서비스 팩, 커널 개체, 드라이버, 서비스, Internet Explorer 확장, 인쇄 확장, Windows Explorer 확장, 다운로드한 프로그램 파일, 활성 설치 요소, 제어판 애플릿, 호스트 및 레지스트리 기록, IP 주소, 브라우저 유형, 이메일 클라이언트, 카스퍼스키 랩 제품 버전 번호 등 일반적이지만 개인을 식별할 수 없는 하드웨어 및 소프트웨어에 대한 정보;
    - 카스퍼스키 랩 제품에서 생성한 것으로 사용자를 식별하지 않고 개인 시스템만 식별하며 개인 정보가 포함되어 있지 않은 고유 ID;
    - 컴퓨터의 안티 바이러스 감시 상태에 대한 정보, 악성 프로그램으로 의심되는 모든 파일 또는 활동에 대한 데이터(예: 바이러스 이름, 탐지 날짜/시간, 감염 파일의 이름/경로 및 크기, 네트워크 공격의 IP 및 포트,

악성 프로그램으로 의심되는 프로그램의 이름 등) 위에서 참조한 수집 데이터는 개인 식별 정보를 포함하지 않습니다.

- 확장 데이터:
  - 사용자가 다운로드하여 디지털로 서명한 프로그램에 대한 정보(예: URL, 파일 크기, 서명자 이름 등)
  - 실행 프로그램에 대한 정보(예: 크기, 속성, 생성 날짜, PE 헤더에 대한 정보, 지역, 이름, 위치, 사용된 압축 유틸리티 등)

  카스퍼스키 시큐리티 네트워크 서비스는 추가 검사를 위해 파일 전체 및/또는 일부를 수집하여 카스퍼스키 랩에 제출할 수 있습니다. 사용자가 카스퍼스키 랩 데이터 수집 정책을 수락한 경우에만 파일 전체 및/또는 일부를 전송할 수 있습니다.

안전한 데이터 전송 및 보관

카스퍼스키 랩은 수집한 정보의 보안을 유지하기 위해 최선을 다합니다. 수집한 정보는 컴퓨터 서버에 보관되며 접근이 제한되고 제어됩니다. 카스퍼스키 랩은 업계 표준 방어벽 및 암호 보호 시스템에 의해 보호되는 안전한 데이터 네트워크를 작동합니다. 카스퍼스키 랩은 광범위한 보안 기술 및 절차를 사용하여 수집한 정보를 무단 접근, 사용, 공개 등과 같은 보안위협으로부터 보호합니다. 카스퍼스키 랩의 보안 정책은 정기적으로 검토되고 필요할 경우 개정되며 권한이 있는 개인만 수집한 데이터에 접근할 수 있습니다. 카스퍼스키 랩은 본 정책에 따라 사용자 정보를 안전하게 취급하기 위한 조치를 취합니다. 그러나 모든 데이터 전송의 보안을 보장할 수는 없습니다. 결과적으로 카스퍼스키 랩은 개인 데이터를 보호하기 위해 노력하지만 사용자가 카스퍼스키 랩에 전송하는 모든 데이터 또는 카스퍼스키 시큐리티 네트워크 등 카스퍼스키 랩의 제품 또는 서비스에 대한 모든 데이터의 보안을 보장할 수 없습니다. 이러한 모든 서비스의 사용은 전적으로 사용자의 책임입니다.

수집한 데이터는 카스퍼스키 랩 서버로 전송될 수 있으며 카스퍼스키 랩은 수집한 정보가 전송될 경우 적합한 수준의 보호 조치를 받도록 하기 위해 필요한 예방 조치를 취했습니다. 카스퍼스키 랩은 수집한 데이터를 기밀 정보로 취급하며, 따라서 기밀 정보의 보호 및 사용과 관련한 당사 보안 절차 및 기업 정책을 준수합니다. 수집한 데이터가 카스퍼스키 랩에 도달하면 해당 데이터는 카스퍼스키 랩 외부에서의 무단 접근을 차단하기 위해 고안된 로그인/암호 절차 및 전자 방어벽을 활용하는 등 업계 관례대로 물리적 및 전자적 보안 기능을 지닌 서버에 보관됩니다. 본 정책이 적용되는 카스퍼스키 시큐리티 네트워크에서 수집한 데이터는 미국 및 기타 관할 지역과 카스퍼스키 랩이 비즈니스를 수행하는 기타 국가에서 처리 및 보관됩니다. 모든 카스퍼스키 랩 직원은 당사의 보안 정책을 숙지하고 있습니다. 사용자 데이터는 업무를 수행하기 위해 필요한 직원만 접근이 허용됩니다. 저장된 모든 데이터는 개인 식별 정보와 연관이 없습니다. 카스퍼스키 랩은 카스퍼스키 시큐리티 네트워크에서 보관하고 있는 데이터를 카스퍼스키 랩에서 홍보 또는 기타 목적으로 수집한 데이터, 연락처 목록 또는 구독 정보와 통합하지 않습니다.

C. 수집 데이터의 사용

개인 정보 사용 방법

카스퍼스키 랩에서 데이터를 수집하는 목적은 잠재적인 보안 위험이 있는 소스를 분석 및 식별하고, 카스퍼스키 랩의 제품에서 악의적인 동작, 사기성 웹사이트, 크라임웨어 및 기타 인터넷 보안위협을 탐지하는 기능을 향상시켜 향후 카스퍼스키 랩 고객에게 최고 수준의 보호 기능을 제공하기 위한 것입니다.

제 3 자에 정보 공개

카스퍼스키 랩은 법에서 요구하거나 허용한 대로 또는 법률 소환장이나 기타 소송 절차에 대한 대응으로 사법 당국자가 그렇게 하도록 요청한 경우, 또는 해당 법률, 규정, 법률 소환장, 기타 소송 절차 또는 강제적인 정부 요청을 준수하기 위해 그렇게 하기로 요청받은 경우 수집한 정보를 공개할 수 있습니다. 또한 카스퍼스키 랩은 개인 식별 정보의 공개가 본 정책 또는 회사와 사용자 간의 협약 조건을 위반할 소지가 있는 사람을 식별하거나 연락을 하거나 기타 법률적 조치를 취하는 데 필요하다고 판단된 경우, 또는 카스퍼스키 시큐리티 네트워크의 개발, 동작 및 유지 관리 시 당사를 지원하는 특정 제 3 자와의 기밀성 및 라이센스 협약에 의거하여 사용자 및 공공의 안전을 보호하기 위해 필요하다고 판단된 경우 해당 정보를 공개할 수 있습니다. 인터넷 보안 위험에 대한 인식을 조성하고 탐지 및 방지 가능성을 높이기 위해 카스퍼스키 랩은 특정 정보를 리서치 조직 및 기타 보안 소프트웨어 공급사와 공유할 수 있습니다. 또한 카스퍼스키 랩은 수집된 정보를 기반으로 산출된 통계를 활용하여 보안 위험 동향을 추적하여 관련 리포트를 게시할 수 있습니다.

선택 사항

카스퍼스키 시큐리티 네트워크에 참여하는 것은 사용자의 선택 사항입니다. 카스퍼스키 랩 제품의 옵션 페이지에 있는 피드백 설정에서 언제든지 카스퍼스키 시큐리티 네트워크 서비스를 활성화 및 비활성화할 수 있습니다. 그러나 카스퍼스키 시큐리티 네트워크 서비스를 비활성화하기로 선택한 경우 이 데이터의 수집에 따른 일부 서비스를 제공하지 않을 수 있습니다. 카스퍼스키 랩 제품의 서비스 기간이 종료되어도 카스퍼스키 랩 소프트웨어의 일부 기능은 계속 실행 가능할 수 있지만 수집 정보는 카스퍼스키 랩에 더이상 자동으로 전송되지 않습니다.

또한 카스퍼스키 랩은 사용자가 이전에 가입한 서비스의 사용에 영향을 미칠 수 있는 특정 변경 사항을 사용자에게 알려드리기 위해 간헐적으로 알림 메시지를 사용자에게 전송할 권한을 보유합니다. 또한 합법적인 절차의 일부로 그렇게 하도록 요청받은 경우 또는 해당 라이센스, 보증 및 구입 협약을 위반한 경우 사용자에게 연락할 수 있는 권한을 보유합니다.

카스퍼스키 랩은 법률과 관련하여 또는 사용자에게 중요할 수 있는 사안과 관련하여 사용자에게 연락할 수 있는 권한이 필요하다고 판단한 경우 그러한 권한을 보유합니다. 이러한 권한을 보유했더라도 사용자가 그렇게 하지 않도록 요청한 경우에는 새로운 서비스 또는 기존 서비스를 판매할 목적으로 사용자에게 연락을 취할 수 없습니다. 이러한 종류의 통신문을 발송하는 것은 흔하지 않은 일입니다

.

D. 데이터 수집 – 관련 문의 및 불만 사항

카스퍼스키 랩은 사용자의 데이터 수집 관련 문의 사항을 최선을 다해 해결하려고 노력합니다. 사용자의 정보 또는 데이터와 관련하여 본 정책을 준수하지 않는 경우가 있다고 판단되면 카스퍼스키 랩에 이메일(support@kaspersky.co.kr)을 통해 알려주시기 바랍니다.

메일에 문의 내용을 최대한 자세히 설명해 주십시오. 카스퍼스키 랩은 문의 및 불만 사항에 대한 조사를 즉시 착수할 것입니다.

정보 제공은 강제성이 없습니다. 사용자는 언제든지 해당 카스퍼스키 제품의 "설정" 페이지에 있는 "피드백" 섹션에서 데이터 수집 옵션을 해제할 수 있습니다.

Copyright ⓒ 2009 Kaspersky Lab. All rights reserved

타사 코드 사용

카스퍼스키 안티 바이러스 개발 중에는 다음과 같은 타사 코드가 사용되었습니다.

참조:

Crypto C library (데이터 시큐리티 소프트웨어 라이브러리) 182

Fastscript 1.9 라이브러리 182

Libnkfm 7.4.7.7 라이브러리 182

GNU bison parser 라이브러리 183

AGG 2.4 라이브러리 183

OpenSSL 0.9.8d 라이브러리 184

Gecko SDK 1.8 라이브러리 185

Zlib 1.2 라이브러리 186

Libpng 1.2.8, 1.2.29 라이브러리 186

Libnkfm 2.0.5 라이브러리 186

Expat 1.2, 2.0.1 라이브러리 186

Info-ZIP 5.51 라이브러리 186

Windows Installer XML (WiX) 2.0 라이브러리 187

Passthru 라이브러리 191

Filter 라이브러리 191

Netcfg 라이브러리 191

Pcre 3.0 라이브러리 191

RFC1321-based (RSA-free) MD5 라이브러리 191

Windows Template Library (WTL 7.5) 191

Libjpeg 6b 라이브러리 195

Libungif 3.0 라이브러리 196

Libxdr 라이브러리 197

Tiniconv - 1.0.0 라이브러리 197

Bzip2/libbzip2 1.0.5 라이브러리 204

Libspf2-1.2.9 라이브러리 204

Protocol Buffer 라이브러리 205

CRYPTO C LIBRARY (데이터 시큐리티 소프트웨어 라이브러리)

디지털 서명을 생성하고 확인하기 위해서, CryptoEx LLC, http://www.cryptoex.ru 에서 개발한 Crypto C 데이터 시큐리티 소프트웨어 라이브러리를 사용합니다.

FASTSCRIPT 1.9 라이브러리

FastScript 라이브러리를 프로그램을 개발할 때 사용되었습니다. Copyright © Fast Reports Inc. All rights reserved.

LIBNKFM 7.4.7.7 라이브러리

카스퍼스키 안티 바이러스 개발 시 Pcre 7.4 라이브러리가 사용되었습니다. Library pcre 7.4 copyright ⓒ 1997-2008 University of Cambridge, BSD 사용 허가서

PCRE 는 정규식을 지원하는 라이브러리 함수로서 구문 및 의미 체계가 Perl 5 언어와 매우 유사합니다.

PCRE 릴리스 5 는 아래 설명된 "BSD" 사용 허가서에 따라 배포됩니다. PCRE 관련 문서는 "doc" 디렉터리에 제공되며 소프트웨어와 동일한 조항에 따라 배포됩니다.

저작자: Philip Hazel <ph10@cam.ac.uk>

University of Cambridge Computing Service,

Cambridge, England. 전화: +44 1223 334714.

수정 여부와 상관 없이 소스 및 이진 형식으로 배포하거나 사용하는 것은 다음 조건을 충족할 경우에 한해 허용됩니다

- 소스 코드로 배포할 경우 위의 저작권 표시, 본 조건 목록 및 다음 고지 사항을 포함시켜야 합니다.
- 이진 형식으로 배포할 경우 위의 저작권 표시, 본 조건 목록 및 다음 고지 사항을 함께 제공되는 설명서 및/또는 기타 자료에 포함시켜야 합니다.
- 사전 서면 허가 없이는 이 소프트웨어의 2 차적 저작물을 추천 또는 홍보하기 위해 University of Cambridge 이름 또는 해당 기여자 이름을 사용할 수 없습니다.

본 소프트웨어는 저작권자 및 기여자에 의해 "있는 그대로" 제공됩니다. 모든 보증(상품성 및 특정 목적에의 적합성에 대한 묵시적인 보증을 포함하며 이에 제한되지 않음)은 배제됩니다. 저작권자 또는 기여자는 어떠한 경우에도 본 소프트웨어의 사용과 관련하여 발생한 직접, 간접, 부수적, 특별, 징벌적 또는 파생적 손해(대체 제품 또는 서비스의 조달, 사용할 수 없음, 데이터 손실, 영업 이익 손실 또는 영업 중단으로 인한 손해를 포함하되 이에 제한되지 않음)에 대하여 책임을 지지 않습니다. 이는 계약 위반, 엄격 책임, 잘못(과실 포함)인 경우와 그러한 손해의 가능성을 사전에 알고 있던 경우에도 마찬가지입니다.

GNU 분석 라이브러리

카스퍼스키 안티 바이러스 개발 시 특별한 예외 프레임워크 하에 bison parser skeleton 2.3 라이브러리가 사용되었습니다. bison parser skeleton 2.3 copyright ⓒ GNU Project http://ftp.gnu.org/gnu/bison/

특별한 예외로서 GNU 분석 구조의 전부 또는 일부를 포함하는 더 큰 저작물을 만들어 원하는 조항에 따라 배포할 수 있습니다. 단, 해당 저작물이 GNU 분석 구조 또는 그 수정 버전을 사용하는 파서 생성기가 아니어야 합니다. 또한 GNU 분석 구조 자체를 수정하거나 재배포하는 경우 이 특별 예외를 없앨 수도 있습니다. 그 경우 GNU 분석 구조 및 해당 출력 파일은 특별 예외 없이 GNU 일반 공중 사용 허가서에 따라 사용이 허가됩니다.

AGG 2.4 라이브러리

카스퍼스키 안티 바이러스 개발 시 AGG 2.4 라이브러리가 사용되었습니다. AGG (Anti-Grain Geometry) 2.4 copyright ⓒ 2002-2005 Maxim Shemanarev. All rights reserved, 개정된 BSD 사용 허가서

수정 여부와 상관 없이 소스 및 이진 형식으로 배포하거나 사용하는 것은 다음 조건을 충족할 경우에 한해 허용됩니다:

1. 소스 코드로 배포할 경우 위의 저작권 표시, 본 조건 목록 및 다음 고지 사항을 포함시켜야 합니다.
2. 이진 형식으로 배포할 경우 위의 저작권 표시, 본 조건 목록 및 다음 고지 사항을 함께 제공되는 설명서 및/또는 기타 자료에 포함시켜야 합니다.
3. 사전 서면 허가 없이는 이 소프트웨어의 2 차적 저작물을 추천 또는 홍보하기 위해 저작자의 이름을 사용할 수 없습니다

본 소프트웨어는 저작자에 의해 "있는 그대로" 제공됩니다. 모든 보증(상품성 및 특정 목적에의 적합성에 대한 묵시적인 보증을 포함하며 이에 제한되지 않음)은 배제됩니다. 저작자는 어떠한 경우에도 본 소프트웨어의 사용과 관련하여 발생한 직접, 간접, 부수적, 특별, 징벌적 또는 파생적 손해(대체 제품 또는 서비스의 조달, 사용할 수 없음, 데이터 손실, 영업 이익 손실 또는 영업 중단으로 인한 손해를 포함하되 이에 제한되지 않음)에 대하여 책임을 지지 않습니다. 이는 계약 위반, 엄격 책임, 잘못(과실 포함)인 경우와 그러한 손해의 가능성을 사전에 알고 있던 경우에도 마찬가지입니다.

Copyright (c) 2004 Alberto Demichelis

본 소프트웨어는 명시적 또는 묵시적 보증 없이 "있는 그대로" 제공됩니다. 저작자는 어떠한 경우에도 본 소프트웨어의 사용과 관련하여 발생한 손해에 대하여 책임을 지지 않습니다.

다음 제한을 따르는 한 누구든지 본 소프트웨어를 상업적 용도를 포함한 어떠한 용도로도 사용하고 자유롭게 변경 및 재배포할 수 있습니다:

1. 본 소프트웨어의 원 저작자를 올바르게 알려야 합니다. 원 저작자 이외의 누구도 원래 소프트웨어를 저작했다고 주장해서는 안 됩니다. 본 소프트웨어를 제품에 사용하는 경우 제품 설명서에 원 저작자를 밝히는 것이 의무는 아니지만 권장됩니다.

2. 변경된 소스 버전은 이를 명확하게 표시해야 하며 원래 소프트웨어로 오해하게 만들어서는 안 됩니다.

3. 이 고지를 소스 배포 시 제거하거나 변경하면 안 됩니다

OPENSSL 0.9.8D 라이브러리

카스퍼스키 안티 바이러스 개발 시 OpenSSL 0.9.8d 라이브러리가 사용되었습니다. OpenSSL 0.9.8d copyright ⓒ 1998-2007 The OpenSSL Project. All rights reserved, OpenSSL 사용 허가서 및 Original SSLeay 사용 허가서(http://www.openssl.org/).

OpenSSL 사용 허가서

Copyright (c) 1998-2007 The OpenSSL Project. All rights reserved.

수정 여부와 상관 없이 소스 및 이진 형식으로 배포하거나 사용하는 것은 다음 조건을 충족할 경우에 한해 허용됩니다:

1. 소스 코드로 배포할 경우 위의 저작권 표시, 본 조건 목록 및 다음 고지 사항을 포함시켜야 합니다.

2. 이진 형식으로 배포할 경우 위의 저작권 표시, 본 조건 목록 및 다음 고지 사항을 함께 제공되는 설명서 및/또는 기타 자료에 포함시켜야 합니다.

3. 본 소프트웨어의 기능 또는 용도를 언급하는 모든 광고 자료에는 다음 사항을 표시해야 합니다. "본 제품은 OpenSSL Toolkit 에 사용하기 위해 OpenSSL Project 에서 개발한 소프트웨어를 포함합니다. (http://www.openssl.org/)"

4. 사전 서면 허가 없이는 이 소프트웨어의 2 차적 저작물을 추천 또는 홍보하기 위해 "OpenSSL Toolkit" 및 "OpenSSL Project" 이름을 사용할 수 없습니다. 서면 허가를 받으려면 openssl-core@openssl.org 에 문의하십시오.

5. OpenSSL Project 의 사전 서면 허가 없이는 본 소프트웨어의 2 차적 저작물을 "OpenSSL"이라고 칭할 수 없으며 "OpenSSL"을 이름에 표시해서도 안 됩니다.

6. 본 소프트웨어를 어떠한 형태로든 재배포할 경우 다음 사항을 표시해야 합니다. "본 제품은 OpenSSL Toolkit 에 사용하기 위해 OpenSSL Project 에서 개발한 소프트웨어를 포함합니다(http://www.openssl.org/)".

본 소프트웨어는 OpenSSL PROJECT 에 의해 "있는 그대로" 제공됩니다. 모든 보증(상품성 및 특정 목적에의 적합성에 대한 묵시적인 보증을 포함하며 이에 제한되지 않음)은 배제됩니다. OpenSSL PROJECT 또는 관련 기여자는 어떠한 경우에도 본 소프트웨어의 사용과 관련하여 발생한 직접, 간접, 부수적, 특별, 징벌적 또는 파생적 손해(대체 제품 또는 서비스의 조달, 사용할 수 없음, 데이터 손실, 영업 이익 손실 또는 영업 중단으로 인한 손해를 포함하되 이에 제한되지 않음)에 대하여 책임을 지지 않습니다. 이는 계약 위반, 엄격 책임, 잘못(과실 포함)인 경우와 그러한 손해의 가능성을 사전에 알고 있던 경우에도 마찬가지입니다.

본 제품에는 Eric Young(eay@cryptsoft.com)이 저작한 암호화 소프트웨어가 포함되어 있습니다. 본 제품에는 Tim Hudson(tjh@cryptsoft.com)이 저작한 소프트웨어가 포함되어 있습니다.

Original SSLeay 사용 허가서

Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com) All rights reserved.

본 패키지는 Eric Young (eay@cryptsoft.com)이 저작한 SSL 구현물입니다.

본 구현물은 Netscapes SSL 을 준수하도록 저작되었습니다.

본 라이브러리는 다음 조건을 따르는 한 상업적 및 비상업적 용도로 모두 자유롭게 사용할 수 있습니다. 다음 조건은 SSL 코드뿐만 아니라 RC4, RSA, lhash, DES 코드를 비롯한 본 배포에 사용된 모든 코드에 적용됩니다. 본 배포에 포함된 SSL 설명서에는 저작권자가 Tim Hudson(tjh@cryptsoft.com)이라는 점을 제외하고 동일한 저작권 조항이 적용됩니다. 저작권은 여전히 Eric Young 에 있으므로 코드에 있는 저작권 표시를 제거하면 안 됩니다. 본 패키지를 제품에 사용하는 경우 Eric Young 을 사용된 라이브러리 일부의 저작자로 밝혀야 합니다. 이는 프로그램 시작 부분에 텍스트 메시지로 표시해도 되고 패키지에 들어 있는 설명서(온라인 또는 하드카피)에 표시해도 됩니다.

수정 여부와 상관 없이 소스 및 이진 형식으로 배포하거나 사용하는 것은 다음 조건을 충족할 경우에 한해 허용됩니다:

1. 소스 코드로 배포할 경우 저작권 표시, 본 조건 목록 및 다음 고지 사항을 포함시켜야 합니다.
2. 이진 형식으로 배포할 경우 위의 저작권 표시, 본 조건 목록 및 다음 고지 사항을 함께 제공되는 설명서 및/또는 기타 자료에 포함시켜야 합니다.
3. 본 소프트웨어의 기능 또는 용도를 언급하는 모든 광고 자료에는 다음 사항을 표시해야 합니다. "본 제품에는 Eric Young(eay@cryptsoft.com)이 저작한 암호화 소프트웨어가 포함되어 있습니다." 사용하는 라이브러리의 루틴이 암호화와 관련되지 않은 경우 "암호화"라는 용어는 생략해도 무방합니다.
4. 프로그램 디렉터리(프로그램 코드)에서 Windows 관련 코드(또는 2 차적 저작물)를 포함하는 경우 다음 사항을 표시해야 합니다. 본 제품에는 Tim Hudson(tjh@cryptsoft.com)이 제작한 소프트웨어가 포함되어 있습니다.

본 소프트웨어는 Eric Young 에 의해 "있는 그대로" 제공됩니다. 모든 보증(상품성 및 특정 목적에의 적합성에 대한 묵시적인 보증을 포함하며 이에 제한되지 않음)은 배제됩니다. 저작자 또는 기여자는 어떠한 경우에도 본 소프트웨어의 사용과 관련하여 발생한 직접, 간접, 부수적, 특별, 징벌적 또는 파생적 손해(대체 제품 또는 서비스의 조달, 사용할 수 없음, 데이터 손실, 영업 이익 손실 또는 영업 중단으로 인한 손해를 포함하되 이에 제한되지 않음)에 대하여 책임을 지지 않습니다. 이는 계약 위반, 엄격 책임, 잘못(과실 포함)인 경우와 그러한 손해의 가능성을 사전에 알고 있던 경우에도 마찬가지입니다.

본 코드의 공개 버전 또는 2 차적 저작물에 대한 사용 허가서 및 배포 조항은 변경할 수 없습니다. 즉, 본 코드를 다른 배포 사용 허가서(GNU 공중 사용 허가서 포함)에 따라 단순히 복사해 놓을 수 없습니다

GECKO SDK 1.8 라이브러리

카스퍼스키 안티 바이러스 개발 시 Gecko SDK 1.8 라이브러리가 사용되었습니다. Gecko SDK 1.8 Copyright © Mozilla Foundation. All rights reserved, MPL 1.1 사용 허가서(http://www.mozilla.org/MPL/MPL-1.1.html). 배포 패키지 웹사이트 및 링크: http://developer.mozilla.org/en/docs/Gecko_SDK

ZLIB 1.2 라이브러리

카스퍼스키 안티 바이러스 개발 시 Zlib 1.2 라이브러리가 사용되었습니다. zlib 1.2 copyright © 1995-2005 Jean-loup Gailly and Mark Adler All rights reserved, zlib/libpng 사용 허가서

LIBPNG 1.2.8, 1.2.29 라이브러리

카스퍼스키 안티 바이러스 개발 시 libpng 1.2.8, 1.2.29 라이브러리가 사용되었습니다. libpng 1.2.8, 1.2.29 copyright © 2004, 2006-2008 Glenn Randers-Pehrson. All rights reserved, zlib/libpng 사용 허가서

LIBNKFM 2.0.5 라이브러리

카스퍼스키 안티 바이러스 개발 시 libnkfm 2.0.5 라이브러리가 사용되었습니다. libnkfm 2.0.5 Copyright (c) KUBO Takehiro. All rights reserved.

EXPAT 1.2, 2.0.1 라이브러리

카스퍼스키 안티 바이러스 개발 시 Expat 1.2, 2.0.1 라이브러리가 사용되었습니다. Expat 1.2, 2.0.1 Copyright (c) 1998, 1999, 2000 Thai Open Source Software Center Ltd. All rights reserved, 다음 조건에 따라 사용

다음 조건을 따르는 한 본 소프트웨어 및 관련 설명서 파일("소프트웨어")을 수령하는 사람은 누구든지 소프트웨어를 사용, 복제, 수정, 병합, 게시, 배포, 2 차적 권한 부여, 판매하고 소프트웨어를 제공할 사람에게 같은 권한을 부여할 권리를 제한 없이 가집니다.

위의 저작권 표시 및 본 사용 허가 공지는 소프트웨어의 모든 복제본 또는 주요 일부분에 포함해야 합니다.

특정 목적에 대한 적합성이나 상업성 여부에 대한 보증을 포함한 어떠한 형태의 명시적 또는 묵시적 보증도 없이 "있는 그대로" 본 소프트웨어를 제공합니다. 저작자 또는 저작권자는 어떠한 경우에도 본 소프트웨어의 사용과 관련하여 발생한 청구, 손해 등에 대하여 책임을 지지 않습니다. 이는 계약 위반, 잘못의 경우에도 마찬가지입니다.

INFO-ZIP 5.51 라이브러리

카스퍼스키 안티 바이러스 개발 시 Info-ZIP 5.51 라이브러리가 사용되었습니다. Info-ZIP 5.51 Copyright (c) 1990-2007. All rights reserved, Info-ZIP 사용 허가서

본 소프트웨어는 명시적 또는 묵시적 보증을 포함한 어떠한 보증도 없이 "있는 그대로" 제공됩니다. Info-ZIP 또는 관련 기여자는 어떠한 경우에도 본 소프트웨어를 사용하거나 사용하지 못함으로 인한 직접, 간접, 부수적, 특별, 파생적 손해에 대하여 책임을 지지 않습니다.

위의 고지 사항 및 다음 제한을 따르는 한 누구든지 본 소프트웨어를 상업적 용도를 포함한 어떠한 용도로도 사용하고 자유롭게 변경 및 재배포할 수 있습니다.

1. 소스 코드를 전부 또는 일부 재배포할 경우 위의 저작권 표시, 정의, 고지 사항 및 다음 조건 목록을 포함시켜야 합니다.

2. 이진 형식(컴파일된 실행물 및 라이브러리)으로 배포할 경우 위의 저작권 표시, 정의, 고지 사항 및 본 조건 목록을 함께 제공되는 설명서 및/또는 기타 자료에 포함시켜야 합니다. 이 조건에 대한 예외가 성립되는 경우는 오직 표준 UnZipSFX 이진 형식(SFXWiz 포함)을 자동 압축 풀기 압축 파일의 일부로 재배포하는 경우입니다. 이진 형식에서 일반 SFX 배너를 제거하거나 중지하지 않는 한 본 사용 허가서를 포함하지 않고도 이것이 허용됩니다.

3. 새로운 운영 체제 포트, 새로운 그래픽 인터페이스를 사용한 기존 포트, 수정 또는 추가된 기능이 있는 버전, Info-ZIP 이외에서 만든 동적/공유/정적 라이브러리 버전을 포함하나 이에 제한되지 않는 변경된 버전은 이 사실을 명확하게 표시해야 하며 원래 소스로 오해하거나 이진 형식의 경우 원래 소스에서 컴파일된 것으로 오해하게 만들어서는 안 됩니다. 또한 그러한 변경된 버전은 Info-ZIP 의 명시적인 허가 없이 변경된 버전에 "Info-ZIP" 이름(또는 대소문자 변경을 비롯한 기타 변형된 형태), "Pocket UnZip," "WiZ" 또는 "MacZip"을 표시하지 않는 것을 포함하나 이에 제한되지 않고 Info-ZIP 릴리스로 오해하게 만들어서는 안 됩니다. 또한 Info-ZIP 이 변경된 버전을 지원하는 것처럼 비쳐질 수 있으므로 변경된 버전에는 Zip-Bugs 또는 Info-ZIP 이메일 주소나 Info-ZIP URL 을 사용해서는 안 됩니다.

4. Info-ZIP 은 "Info-ZIP," "Zip," "UnZip, "UnZipSFX," "WiZ," "Pocket UnZip," "Pocket Zip" 및 "MacZip" 이름을 자체 소스 및 이진 형식 릴리스에 사용할 수 있는 권리를 보유합니다.

WINDOWS INSTALLER XML (WIX) 2.0 LIBRARY

카스퍼스키 안티 바이러스 개발 시 Windows Installer XML (WiX) 2.0 이 사용되었습니다. Windows Installer XML (WiX) 2.0 Copyright (c) 2005 Microsoft Corporation. All rights reserved, CPL 1.0 라이센스(http://sourceforge.net/projects/wix/)

Common Public License 버전 1.0

해당 프로그램은 본 Common Public License("사용 허가서") 조건에 따라 제공됩니다. 프로그램 사용, 복제 또는 배포는 본 사용 허가서에 대한 동의로 간주됩니다.

1. 정의

"기여물"은 다음을 의미합니다.

1) 초기 기여자의 경우, 본 사용 허가서에 따라 배포된 초기 코드 및 문서

2) 이후 각 기여자의 경우

i) 프로그램에 대한 변경물

ii) 프로그램에 대한 추가물

여기서 프로그램에 대한 변경물과 추가물은 해당 기여자에 의해 기원되고 배포됩니다. 기여자 자신 또는 기여자의 대리인에 의해 추가된 경우 기여물이 기여자로부터 '기원'되었다고 합니다. 다음과 같은 프로그램

추가물은 기여물에 포함되지 않습니다. (i) 자체 사용 허가서에 따라 프로그램과 결합되어 배포된 별도 소프트웨어 모듈 (ii) 프로그램의 2 차적 저작물이 아닌 것

"기여자"는 프로그램을 배포하는 개인 또는 주체를 의미합니다.

"공인된 특허"는 기여자가 사용을 허가할 수 있는 특허권으로서, 기여물 단독으로 또는 프로그램과 결합되어 사용되거나 판매될 경우 침해됩니다.

"프로그램"은 본 사용 허가서에 따라 배포되는 기여물을 의미합니다.

"수령인"은 모든 기여자를 포함하여 본 사용 허가서에 따라 프로그램을 수령하는 사람을 의미합니다.

2. 권리 부여

1) 본 사용 허가서 조항에 따라 각 기여자는 수령인에게 해당 기여자의 기여물 및 2 차적 저작물을 소스 코드와 목적 코드 형태로 복제, 2 차적 저작물 준비, 공개적 전시, 공개적 실행, 배포 및 2 차 권한 부여를 위한 비배타적이고 전 세계적이며 사용료가 없는 저작권 사용 허가를 부여합니다.

2) 본 사용 허가서 조항에 따라 각 기여자는 수령인에게 기여자의 기여물을 소스 코드와 목적 코드 형태로 저작, 사용, 판매, 판매 제안, 수입 또는 기타 전송을 위한 비배타적이고 전 세계적이며 사용료가 없는 공인된 특허의 특허 사용 허가를 부여합니다. 이 특허 사용 허가는 기여물이 기여자에 의해 추가될 때 기여물과 프로그램의 결합물에 적용됩니다. 이러한 기여물의 추가를 통해 결합물은 공인된 특허로 보호됩니다. 특허 사용 허가는 기여물을 포함하는 기타 결합물에는 적용되지 않습니다. 어떤 하드웨어도 본 사용 허가서에 의해 사용이 허가되지 않습니다.

3) 각 기여자가 여기에 명시된 기여물에 대한 사용을 허가하더라도 수령인은 프로그램이 어떤 주체의 특허 또는 다른 지적재산권을 침해하지 않는다는 어떠한 보증도 각 기여자에 의해 제공되지 않는다는 점을 인지해야 합니다. 각 기여자는 다른 어떤 주체에 의해 제기된 지적재산권 침해 소송과 관련하여 수령인에 대한 모든 책임이 면제됩니다. 본 사용 허가서에 의해 허용된 권리 및 사용 허가를 행사하기 위한 조건으로 각 수령인은 필요한 다른 모든 지적재산권을 보증하는 것에 대해 전적인 책임을 집니다. 예를 들어 수령인이 프로그램을 배포하기 위해 제 3 자의 특허 사용 허가가 필요한 경우 프로그램을 배포하기 전에 사용 허가서를 취득하는 것은 수령인의 책임입니다.

4) 각 기여자는 기여물에서 본 사용 허가서에 명시된 저작권 사용 허가를 부여하기에 충분한 저작권을 갖습니다.

3. 요건

기여자는 자체 사용 허가서에 따라 목적 코드 형태로 프로그램을 배포하려는 경우 다음 사항을 만족해야 합니다.

1) 본 사용 허가서의 규정과 조건을 준수해야 합니다.

2) 자체 사용 허가서는 다음 조건을 만족해야 합니다.

i) 모든 기여자 측면에서 권리와 비침해의 보증 또는 조건을 포함한 모든 명시적/묵시적 보증과 조건, 특정 목적에의 적합성 및 상업성의 묵시적 보증 또는 조건을 실제적으로 포기합니다.

ii) 모든 기여자의 측면에서 이익 손실과 같은 직접적, 간접적, 특수적, 우발적 및 필연적 손해를 포함한 손해에 대한 모든 책임을 실제적으로 배제합니다.

iii) 본 사용 허가서와 다른 모든 조항은 기타 당사자가 아닌 기여자 자신이 제공함을 명시합니다.

iv) 기여자가 프로그램의 소스 코드를 제공함을 명시하고, 소프트웨어 교환을 위해 통상적으로 사용되는 매체를 통해 또는 다른 적절한 방법으로 소스 코드를 얻는 방법을 사용자에게 알려 줍니다.

프로그램이 소스 코드 형태로 제공되는 경우 다음 조건을 만족해야 합니다.

1) 프로그램은 본 사용 허가서에 따라 제공해야 합니다.

2) 각 프로그램 복제본에는 본 사용 허가서의 복제본을 포함해야 합니다.

기여자는 프로그램에 포함된 저작권 표시를 제거하거나 변경할 수 없습니다.

각 기여자는 이후 수령인이 기여물의 창작자를 적절하게 알 수 있도록 기여물의 창작자로서 자신을 알려야 합니다.

4. 상업적 배포

소프트웨어의 상업적 배포자는 사용자, 비즈니스 파트너 등에 관한 특정 책임을 수용할 수 있습니다. 프로그램의 상업적 사용을 용이하게 하는 것이 본 사용 허가서의 목적이지만, 기여자는 상업적 제품에 프로그램을 포함할 경우 다른 기여자를 잠재적으로 불리하게 만들지 않아야 합니다. 따라서 기여자가 상업적 제품에 프로그램을 포함한다면 그러한 기여자("상업적 기여자")는 상업적 제품에 포함된 프로그램 배포와 관련하여 상업적 기여자의 행동 또는 태만으로 인한 경우 제 3 자에 의한 청구, 소송 및 다른 법적 활동으로 발생하는 모든 손실, 손해 및 비용(총체적으로 "손실")에 대해 모든 다른 기여자("면책 기여자")를 변호하고 면책해야 합니다. 이 조항에서의 의무는 실제적 또는 추정적 지적재산권 침해와 관계된 모든 청구 또는 손실에는 적용되지 않습니다. 면책 기여자는 면책을 받기 위해 다음과 같은 조건을 만족해야 합니다. 1) 그러한 청구 사실에 대해 상업적 기여자에게 서면으로 즉시 공지하고 2) 상업적 기여자가 변호 및 관련 화해 협상을 주도하도록 하며 이를 위해 상업적 기여자에게 협조해야 합니다. 면책 기여자는 자신의 비용을 들여 그러한 청구를 처리하는 데 참여할 수 있습니다.

예를 들어 기여자는 상업적 제품인 X 제품에 프로그램을 포함할 수 있습니다. 그러면 이 기여자는 상업적 기여자입니다. 이 상업적 기여자가 X 제품과 관계된 성능 설명 또는 보증을 제공하는 경우 그러한 성능 설명 및 보증은 이 상업적 기여자의 전적인 책임입니다. 이 조항에 따라 상업적 기여자는 그러한 성능 설명 및 보증과 관련하여 다른 기여자에 대해 청구가 제기될 경우 이를 변호해야 합니다. 그리고 법정이 다른 기여자에게 성능 설명 및 보증과 관련한 손해를 보상하라고 요구할 경우 상업적 기여자가 해당 손해 비용을 지불해야 합니다.

5. 보증 없음

본 사용 허가서에 명시된 경우를 제외하고, 프로그램은 특정 목적에의 적합성 또는 권리, 비침해, 상업성에 대한 어떠한 보증 또는 조건을 포함한 명시적 또는 묵시적으로 포함된 모든 종류의 보증 또는 조건 없이 "있는 그대로" 제공됩니다. 각 수령인은 프로그램의 사용 및 배포의 타당성을 결정함에 있어 전적인 책임을 집니다. 또한 각 수령인은 본 사용 허가서에 따른 권리 행사와 관련된 모든 위험을 감수해야 합니다. 그러한

위험에는 프로그램 오류, 관련 법률 준수, 데이터/프로그램/장비 손상 또는 손실, 작동 불가 또는 중단 등의 위험 및 비용이 포함됩니다.

6. 책임 면제

본 사용 허가서에 명시된 경우를 제외하고, 수령인과 기여자는 모든 직접적, 간접적, 우발적, 특수적, 전형적 또는 필연적 손해(이익 손실 포함)에 대해 어떠한 책임도 지지 않습니다. 비록 그 손해의 가능성을 알고 있었다 하더라도 그 원인 또는 책임론에 관계없이 프로그램의 사용/배포 또는 본 사용 허가서에 의한 권리 행사로 발생한 계약, 무과실 책임, 불법 행위(부주의 포함)에 대해 책임을 지지 않습니다.

7. 일반 사항

본 사용 허가서의 어떤 조항이 준거법에 따라 유효하지 않거나 적용될 수 없는 경우에도 본 사용 허가서의 나머지 조항의 유효성 또는 적용성에 영향을 미치지 않습니다. 또한 해당 조항을 개정할 경우 본 사용 허가서 당사자들의 추가적 활동 없이 조항을 유효하고 적용 가능하게 만드는 데 필요한 최소한도로만 개정해야 합니다.

수령인이 소프트웨어에 적용되는 특허와 관련하여 기여자에게 특허 소송(상호 소송 또는 맞고소 포함)을 시작하는 경우 본 사용 허가서에 의해 기여자가 수령인에게 부여한 특허 사용 허가는 소송 제기일에 소멸됩니다. 또한 수령인이 프로그램 자체(다른 소프트웨어 또는 하드웨어와 프로그램의 결합물은 제외)가 수령인의 특허를 침해함을 주장하며 특정 주체에 대해 특허 소송(상호 소송 또는 맞고소 포함)을 시작하는 경우 제 2 조 (2)항에 따라 부여된 수령인의 권리는 소송 제기일에 소멸됩니다.

본 사용 허가서에 따른 모든 수령인의 권리는 본 사용 허가서의 구체적 조항을 따르지 않고 그러한 불이행을 인지한 후 합리적인 기간 내에 시정하지 않는 경우 소멸됩니다. 본 사용 허가서에 따른 모든 수령인의 권리가 소멸되는 경우 수령인은 프로그램의 사용 및 배포를 가능한 한 즉시 중지해야 합니다. 그러나 본 사용 허가서에 따른 수령인의 의무와 프로그램과 관련하여 수령인에게 부여된 모든 사용 허가는 계속 유효합니다.

본 사용 허가서 복제본은 누구나 복제 및 배포할 수 있습니다. 그러나 불일치를 피하기 위해 본 사용 허가서는 저작권을 가지며 다음 방식으로만 수정할 수 있습니다. 사용 허가서 관리자는 때때로 본 사용 허가서의 새로운 버전(개정 포함)을 공표할 권리는 가집니다. 사용 허가서 관리자를 제외한 어떤 당사자도 본 사용 허가서를 수정할 수 없습니다. IBM 은 원래 사용 허가서 관리자이며 사용 허가서 관리자 책임을 적절한 별도 주체에게 위임할 수 있습니다. 본 사용 허가서의 각 새 버전에는 고유한 버전 번호가 부여됩니다. 프로그램(기여물 포함)은 반드시 프로그램을 수령할 때의 사용 허가서 버전에 따라서만 배포해야 합니다. 또한 사용 허가서의 새로운 버전이 공표된 후에 기여자는 새로운 버전에 따라 프로그램(기여물 포함)을 배포할지 여부를 선택할 수 있습니다. 위 제 2 조 (1)항 및 제 2 조 (2)항에 명시된 경우를 제외하고, 수령인은 명시, 묵시, 금반어 또는 기타 방법에 의한 경우이든 관계없이 본 사용 허가서에 따른 모든 기여자의 지적재산권에 대해 어떠한 권리 또는 사용 허가도 받을 수 없습니다. 본 사용 허가서에 의해 명시적으로 부여되지 않은 프로그램의 모든 권리는 유보됩니다.

본 사용 허가서는 미국 지적재산권 법 및 뉴욕주 법에 준거합니다. 본 사용 허가서에 대해 어떠한 당사자도 행위 원인 발생 후 1 년 이상 지난 후에는 본 사용 허가서에 따른 법적 절차를 진행할 수 없습니다. 각 당사자는 소송에서 배심원 공판을 위한 권리를 포기합니다.

PASSTHRU 라이브러리

카스퍼스키 안티 바이러스 개발 시 Ndis Intermediate Miniport 드라이버 샘플 라이브러리가 사용되었습니다. Ndis Intermediate Miniport driver sample Copyright (c) 1992-2000 Microsoft Corporation. All rights reserved.

FILTER 라이브러리

카스퍼스키 안티 바이러스 개발 시 Ndis Sample NDIS Lightweight 필터 드라이버 라이브러리가 사용되었습니다. Ndis Sample NDIS Lightweight filter driver Copyright (c) 2004-2005 Microsoft Corporation. All rights reserved.

NETCFG 라이브러리

카스퍼스키 안티 바이러스 개발 시 Network Configuration Sample 라이브러리가 사용되었습니다. Network Configuration Sample Copyright (c) 1997 Microsoft Corporation. All rights reserved.

PCRE 3.0 라이브러리

카스퍼스키 안티 바이러스 개발 시 Pcre 3.0 라이브러리가 사용되었습니다. pcre 3.0 copyright ⓒ 1997-1999 University of Cambridge, PCRE 사용 허가서. All rights reserved.

RFC1321-BASED (RSA-FREE) MD5 라이브러리

카스퍼스키 안티 바이러스 개발 시 RFC1321 기반(RSA 없음) MD5 라이브러리가 사용되었습니다. Copyright (c) 1999, 2002 Aladdin Enterprises. All rights reserved. zlib/libpng 사용 허가서에 따라 배포

WINDOWS TEMPLATE 라이브러리 (WTL 7.5)

카스퍼스키 안티 바이러스 개발 시 Windows Template Library 7.5 가 사용되었습니다. Windows Template Library 7.5 Copyright (c)2005 Microsoft Corporation. All rights reserved, Common Public License 1.0, http://sourceforge.net/projects/wtl/

Common Public License 버전 1.0

해당 프로그램은 본 Common Public License("사용 허가서") 조건에 따라 제공됩니다. 프로그램 사용, 복제 또는 배포는 본 사용 허가서에 대한 동의로 간주됩니다.

1. **정의**

"기여물"은 다음을 의미합니다.

1) 초기 기여자의 경우, 본 사용 허가서에 따라 배포된 초기 코드 및 문서

2) 이후 각 기여자의 경우

i) 프로그램에 대한 변경물

ii) 프로그램에 대한 추가물

여기서 프로그램에 대한 변경물과 추가물은 해당 기여자에 의해 기원되고 배포됩니다. 기여자 자신 또는 기여자의 대리인에 의해 추가된 경우 기여물이 기여자로부터 '기원'되었다고 합니다. 다음과 같은 프로그램 추가물은 기여물에 포함되지 않습니다. (i) 자체 사용 허가서에 따라 프로그램과 결합되어 배포된 별도 소프트웨어 모듈 (ii) 프로그램의 2 차적 저작물이 아닌 것

"기여자"는 프로그램을 배포하는 개인 또는 주체를 의미합니다.

"공인된 특허"는 기여자가 사용을 허가할 수 있는 특허권으로서, 기여물 단독으로 또는 프로그램과 결합되어 사용되거나 판매될 경우 침해됩니다.

"프로그램"은 본 사용 허가서에 따라 배포되는 기여물을 의미합니다.

"수령인"은 모든 기여자를 포함하여 본 사용 허가서에 따라 프로그램을 수령하는 사람을 의미합니다.

2. 권리 부여

1) 본 사용 허가서 조항에 따라 각 기여자는 수령인에게 해당 기여자의 기여물 및 2 차적 저작물을 소스 코드와 목적 코드 형태로 복제, 2 차적 저작물 준비, 공개적 전시, 공개적 실행, 배포 및 2 차 권한 부여를 위한 비배타적이고 전 세계적이며 사용료가 없는 저작권 사용 허가를 부여합니다.

2) 본 사용 허가서 조항에 따라 각 기여자는 수령인에게 기여자의 기여물을 소스 코드와 목적 코드 형태로 저작, 사용, 판매, 판매 제안, 수입 또는 기타 전송을 위한 비배타적이고 전 세계적이며 사용료가 없는 공인된 특허의 특허 사용 허가를 부여합니다. 이 특허 사용 허가는 기여물이 기여자에 의해 추가될 때 기여물과 프로그램의 결합물에 적용됩니다. 이러한 기여물의 추가를 통해 결합물은 공인된 특허로 보호됩니다. 특허 사용 허가는 기여물을 포함하는 기타 결합물에는 적용되지 않습니다. 어떤 하드웨어도 본 사용 허가서에 의해 사용이 허가되지 않습니다.

3) 각 기여자가 여기에 명시된 기여물에 대한 사용을 허가하더라도 수령인은 프로그램이 어떤 주체의 특허 또는 다른 지적재산권을 침해하지 않는다는 어떠한 보증도 각 기여자에 의해 제공되지 않는다는 점을 인지해야 합니다. 각 기여자는 다른 어떤 주체에 의해 제기된 지적재산권 침해 소송과 관련하여 수령인에 대한 모든 책임이 면제됩니다. 본 사용 허가서에 의해 허용된 권리 및 사용 허가를 행사하기 위한 조건으로 각 수령인은 필요한 다른 모든 지적재산권을 보증하는 것에 대해 전적인 책임을 집니다. 예를 들어 수령인이 프로그램을 배포하기 위해 제 3 자의 특허 사용 허가가 필요한 경우 프로그램을 배포하기 전에 사용 허가서를 취득하는 것은 수령인의 책임입니다.

4) 각 기여자는 기여물에서 본 사용 허가서에 명시된 저작권 사용 허가를 부여하기에 충분한 저작권을 갖습니다.

3. 요건

기여자는 자체 사용 허가서에 따라 목적 코드 형태로 프로그램을 배포하려는 경우 다음 사항을 만족해야 합니다.

1) 본 사용 허가서의 규정과 조건을 준수해야 합니다.

2) 자체 사용 허가서는 다음 조건을 만족해야 합니다.

i) 모든 기여자 측면에서 권리와 비침해의 보증 또는 조건을 포함한 모든 명시적/묵시적 보증과 조건, 특정 목적에의 적합성 및 상업성의 묵시적 보증 또는 조건을 실제적으로 포기합니다.

ii) 모든 기여자의 측면에서 이익 손실과 같은 직접적, 간접적, 특수적, 우발적 및 필연적 손해를 포함한 손해에 대한 모든 책임을 실제적으로 배제합니다.

iii) 본 사용 허가서와 다른 모든 조항은 기타 당사자가 아닌 기여자 자신이 제공함을 명시합니다.

iv) 기여자가 프로그램의 소스 코드를 제공함을 명시하고, 소프트웨어 교환을 위해 통상적으로 사용되는 매체를 통해 또는 다른 적절한 방법으로 소스 코드를 얻는 방법을 사용자에게 알려 줍니다.

프로그램이 소스 코드 형태로 제공되는 경우 다음 조건을 만족해야 합니다.

1) 프로그램은 본 사용 허가서에 따라 제공해야 합니다.

2) 각 프로그램 복제본에는 본 사용 허가서의 복제본을 포함해야 합니다.

기여자는 프로그램에 포함된 저작권 표시를 제거하거나 변경할 수 없습니다.

각 기여자는 이후 수령인이 기여물의 창작자를 적절하게 알 수 있도록 기여물의 창작자로서 자신을 알려야 합니다.

4. 상업적 배포

소프트웨어의 상업적 배포자는 사용자, 비즈니스 파트너 등에 관한 특정 책임을 수용할 수 있습니다. 프로그램의 상업적 사용을 용이하게 하는 것이 본 사용 허가서의 목적이지만, 기여자는 상업적 제품에 프로그램을 포함할 경우 다른 기여자를 잠재적으로 불리하게 만들지 않아야 합니다. 따라서 기여자가 상업적 제품에 프로그램을 포함한다면 그러한 기여자("상업적 기여자")는 상업적 제품에 포함된 프로그램 배포와 관련하여 상업적 기여자의 행동 또는 태만으로 인한 경우 제 3 자에 의한 청구, 소송 및 다른 법적 활동으로 발생하는 모든 손실, 손해 및 비용(총체적으로 "손실")에 대해 모든 다른 기여자("면책 기여자")를 변호하고 면책해야 합니다. 이 조항에서의 의무는 실제적 또는 추정적 지적재산권 침해와 관계된 모든 청구 또는 손실에는 적용되지 않습니다. 면책 기여자는 면책을 받기 위해 다음과 같은 조건을 만족해야 합니다. 1) 그러한 청구 사실에 대해 상업적 기여자에게 서면으로 즉시 공지하고 2) 상업적 기여자가 변호 및 관련 화해 협상을 주도하도록 하며 이를 위해 상업적 기여자에게 협조해야 합니다. 면책 기여자는 자신의 비용을 들여 그러한 청구를 처리하는 데 참여할 수 있습니다.

예를 들어 기여자는 상업적 제품인 X 제품에 프로그램을 포함할 수 있습니다. 그러면 이 기여자는 상업적 기여자입니다. 이 상업적 기여자가 X 제품과 관계된 성능 설명 또는 보증을 제공하는 경우 그러한 성능 설명 및 보증은 이 상업적 기여자의 전적인 책임입니다. 이 조항에 따라 상업적 기여자는 그러한 성능 설명 및 보증과 관련하여 다른 기여자에 대해 청구가 제기될 경우 이를 변호해야 합니다. 그리고 법정이 다른

기여자에게 성능 설명 및 보증과 관련한 손해를 보상하라고 요구할 경우 상업적 기여자가 해당 손해 비용을 지불해야 합니다.

5. 보증 없음

본 사용 허가서에 명시된 경우를 제외하고, 프로그램은 특정 목적에의 적합성 또는 권리, 비침해, 상업성에 대한 어떠한 보증 또는 조건을 포함한 명시적 또는 묵시적으로 포함된 모든 종류의 보증 또는 조건 없이 "있는 그대로" 제공됩니다. 각 수령인은 프로그램의 사용 및 배포의 타당성을 결정함에 있어 전적인 책임을 집니다. 또한 각 수령인은 본 사용 허가서에 따른 권리 행사와 관련된 모든 위험을 감수해야 합니다. 그러한 위험에는 프로그램 오류, 관련 법률 준수, 데이터/프로그램/장비 손상 또는 손실, 작동 불가 또는 중단 등의 위험 및 비용이 포함됩니다.

6. 책임 면제

본 사용 허가서에 명시된 경우를 제외하고, 수령인과 기여자는 모든 직접적, 간접적, 우발적, 특수적, 전형적 또는 필연적 손해(이익 손실 포함)에 대해 어떠한 책임도 지지 않습니다. 비록 그 손해의 가능성을 알고 있었다 하더라도 그 원인 또는 책임론에 관계없이 프로그램의 사용/배포 또는 본 사용 허가서에 의한 권리 행사로 발생한 계약, 무과실 책임, 불법 행위(부주의 포함)에 대해 책임을 지지 않습니다.

7. 일반 사항

본 사용 허가서의 어떤 조항이 준거법에 따라 유효하지 않거나 적용될 수 없는 경우에도 본 사용 허가서의 나머지 조항의 유효성 또는 적용성에 영향을 미치지 않습니다. 또한 해당 조항을 개정할 경우 본 사용 허가서 당사자들의 추가적 활동 없이 조항을 유효하고 적용 가능하게 만드는 데 필요한 최소한도로만 개정해야 합니다.

수령인이 소프트웨어에 적용되는 특허와 관련하여 기여자에게 특허 소송(상호 소송 또는 맞고소 포함)을 시작하는 경우 본 사용 허가서에 의해 기여자가 수령인에게 부여한 특허 사용 허가는 소송 제기일에 소멸됩니다. 또한 수령인이 프로그램 자체(다른 소프트웨어 또는 하드웨어와 프로그램의 결합물은 제외)가 수령인의 특허를 침해함을 주장하며 특정 주체에 대해 특허 소송(상호 소송 또는 맞고소 포함)을 시작하는 경우 제 2 조 (2)항에 따라 부여된 수령인의 권리는 소송 제기일에 소멸됩니다.

본 사용 허가서에 따른 모든 수령인의 권리는 본 사용 허가서의 구체적 조항을 따르지 않고 그러한 불이행을 인지한 후 합리적인 기간 내에 시정하지 않는 경우 소멸됩니다. 본 사용 허가서에 따른 모든 수령인의 권리가 소멸되는 경우 수령인은 프로그램의 사용 및 배포를 가능한 한 즉시 중지해야 합니다. 그러나 본 사용 허가서에 따른 수령인의 의무와 프로그램과 관련하여 수령인에게 부여된 모든 사용 허가는 계속 유효합니다.

본 사용 허가서 복제본은 누구나 복제 및 배포할 수 있습니다. 그러나 불일치를 피하기 위해 본 사용 허가서는 저작권을 가지며 다음 방식으로만 수정할 수 있습니다. 사용 허가서 관리자는 때때로 본 사용 허가서의 새로운 버전(개정 포함)을 공표할 권리는 가집니다. 사용 허가서 관리자를 제외한 어떤 당사자도 본 사용 허가서를 수정할 수 없습니다. IBM 은 원래 사용 허가서 관리자이며 사용 허가서 관리자 책임을 적절한 별도 주체에게 위임할 수 있습니다. 본 사용 허가서의 각 새 버전에는 고유한 버전 번호가 부여됩니다. 프로그램(기여물 포함)은 반드시 프로그램을 수령할 때의 사용 허가서 버전에 따라서만 배포해야 합니다. 또한 사용 허가서의 새로운 버전이 공표된 후에 기여자는 새로운 버전에 따라 프로그램(기여물 포함)을 배포할지 여부를 선택할 수 있습니다. 위 제 2 조 (1)항 및 제 2 조 (2)항에 명시된 경우를 제외하고, 수령인은 명시, 묵시, 금반어 또는 기타 방법에 의한 경우이든 관계없이 본 사용 허가서에

따른 모든 기여자의 지적재산권에 대해 어떠한 권리 또는 사용 허가도 받을 수 없습니다. 본 사용 허가서에 의해 명시적으로 부여되지 않은 프로그램의 모든 권리는 유보됩니다.

본 사용 허가서는 미국 지적재산권 법 및 뉴욕주 법에 준거합니다. 본 사용 허가서에 대해 어떠한 당사자도 행위 원인 발생 후 1 년 이상 지난 후에는 본 사용 허가서에 따른 법적 절차를 진행할 수 없습니다. 각 당사자는 소송에서 배심원 공판을 위한 권리를 포기합니다.

LIBJPEG 6B 라이브러리

카스퍼스키 안티 바이러스 개발 시 libjpeg 6b 라이브러리가 사용되었습니다. Copyright (c) 1991-1998, Thomas G. Lane. All Rights. 사용 조건은 다음과 같습니다.

법적 사안

일상 용어로 설명 시:

본 소프트웨어의 작동을 보장하지 않습니다. (그러나 버그를 발견하는 경우 알려 주십시오!)

이 소프트웨어는 원하는 용도로 자유롭게 사용할 수 있습니다. 이 소프트웨어는 무료입니다.

이 소프트웨어를 본인이 작성한 것처럼 표시하면 안 됩니다. 프로그램에 사용할 경우 설명서 내에 IJG 코드를 사용했다는 것을 표시해야 합니다.

법적 용어로 설명 시:

저작자는 본 소프트웨어와 해당 품질, 정확도, 상업성, 특정 목적에의 적합성에 대해 어떠한 명시적 또는 묵시적 보증도 제공하지 않습니다. 본 소프트웨어는 "있는 그대로" 제공되며 소프트웨어의 품질 및 정확도와 관련된 모든 위험은 사용자가 부담합니다.

다음 조건을 따르는 한, 비용을 지불하기 않고 어떠한 용도로든 본 소프트웨어를 사용, 복제, 수정 및 배포할 수 있습니다.

(1) 소스 코드의 일부를 배포하는 경우 저작권 표시 및 보증 없음 내용을 변경하지 않고 본 README 파일을 포함해야 합니다. 또한 원래 파일에 대한 추가, 삭제 또는 변경 시 관련 설명서에 이를 명확하게 밝혀야 합니다.

(2) 실행 가능한 코드만 배포하는 경우 관련 설명서에 "본 소프트웨어의 일부는 독립적 JPEG Group 의 저작물에 기반을 둡니다"라는 내용을 표시해야 합니다.

(3) 본 소프트웨어는 사용자가 원치 않는 결과에 대한 책임을 전적으로 수용하는 경우에만 사용이 허가됩니다. 저작자는 어떠한 종류의 손해에도 책임을 지지 않습니다.

이러한 조건은 원 상태의 라이브러리는 물론 IJG 코드에 기반을 둔 모든 소프트웨어 및 2 차적 저작물에 적용됩니다. IJG 의 저작물을 사용하는 경우 이를 밝혀야 합니다.

본 소프트웨어 또는 2 차적 저작물과 관련된 광고 또는 홍보에 IJG 저작자 또는 회사 이름을 사용할 수 없습니다. 본 소프트웨어는 오직 "독립적 JPEG Group 의 소프트웨어"로만 칭해야 합니다.

제품 공급업체가 모든 보증 또는 손해에 대해 책임을 지는 한 본 소프트웨어를 상업적 제품에 사용할 수 있습니다.

본 배포에는 유일한 저작권 소유자인 L. Peter Deutsch(Aladdin Enterprises of Menlo Park, CA)의 허가하에 ansi2knr.c 가 포함되어 있습니다. ansi2knr.c 에는 위의 저작권 및 조건이 적용되지 않고 대신 자유 소프트웨어 재단의 일반적인 배포 조항이 적용됩니다. 주요 내용은 재배포 시 소스 코드를 포함해야 한다는 것입니다. (자세한 내용은 ansi2knr.c 파일 참조) 그러나 ansi2knr.c 는 IJG 코드에서 생성된 프로그램의 일부로는 필요 없으므로 위의 조항에서 언급한 사항 이상의 제한을 부과하지 않습니다.

Unix 구성 스크립트인 "configure"는 GNU Autoconf 를 사용하여 만들어졌습니다. 저작권은 자유 소프트웨어 재단에 있지만 자유롭게 배포 가능합니다. 지원 스크립트(config.guess, config.sub, ltconfig, ltmain.sh)에도 같은 사항이 적용됩니다. 또 다른 지원 스크립트인 install-sh 는 M.I.T 에 저작권이 있지만 자유롭게 배포 가능합니다.

JPEG 규격의 산술 코딩 옵션에는 IBM, AT&T 및 Mitsubishi 가 소유한 특허가 적용됩니다. 따라서 산술 코딩은 하나 이상의 사용 허가서를 얻지 않고는 법적으로 사용이 금지됩니다. 이러한 이유로 산술 코딩 지원은 자유 JPEG 소프트웨어에서 없앴습니다.

(산술 코딩은 특허가 없는 Huffman 모드에 비해 약간의 이점만 갖기 때문에 대다수의 구현물에서는 산술 코딩을 지원하지 않습니다.) 나머지 코드에 대해서는 특허 제한이 없는 것으로

알고 있습니다.

이전에는 IJG 배포에 GIF 파일을 읽고 쓰기 위한 코드가 포함되어 있었습니다. 그러나 Unisys LZW 특허와 관련된 분쟁에 휘말리지 않기 위해 GIF 읽기 지원은 아예 없앴고 GIF 쓰기 지원은 "비압축 GIF"를 생성하도록 간소화했습니다. 이 기법은 LZW 알고리즘을 사용하지 않습니다. 결과 GIF 파일은 보통보다 크지만 모든 표준 GIF 디코더에서 읽을 수 있습니다.

"The Graphics Interchange Format(c)는 CompuServe Incorporated.가 저작권을 갖습니다. GIF(sm)는 CompuServe Incorporated.의 서비스 상표입니다.

LIBUNGIF 3.0 라이브러리

카스퍼스키 안티 바이러스 개발 시 libungif 3.0 라이브러리가 사용되었습니다. Copyright (c) 1997 Eric S. Raymond. 사용 조건은 다음과 같습니다.

다음 조건을 따르는 한 본 소프트웨어 및 관련 설명서 파일("소프트웨어")을 수령하는 사람은 누구든지 소프트웨어를 사용, 복제, 수정, 병합, 게시, 배포, 2 차적 권한 부여, 판매하고 소프트웨어를 제공할 사람에게 같은 권한을 부여할 권리를 제한 없이 가집니다.

위의 저작권 표시 및 본 사용 허가 공지는 소프트웨어의 모든 복제본 또는 주요 일부분에 포함해야 합니다.

특정 목적에 대한 적합성이나 상업성 여부에 대한 보증을 포함한 어떠한 형태의 명시적 또는 묵시적 보증도 없이 "있는 그대로" 본 소프트웨어를 제공합니다. 저작자 또는 저작권자는 어떠한 경우에도 본 소프트웨어의 사용과 관련하여 발생한 청구, 손해 등에 대하여 책임을 지지 않습니다. 이는 계약 위반, 잘못의 경우에도 마찬가지입니다.

LIBXDR 라이브러리

카스퍼스키 안티 바이러스 개발 시 libxdr 라이브러리가 사용되었습니다. libxdr copyright ⓒ Sun Microsystems, Inc. 사용 조건은 다음과 같습니다.

Sun RPC 는 Sun Microsystems, Inc.의 제품이며 모든 테이프 장치 및 소프트웨어 프로그램(전체 또는 일부)의 일부로 이 고지 사항을 포함하는 한 용도 제한 없이 제공됩니다.

사용자는 비용을 지불하지 않고 Sun RPC 를 복제 또는 수정할 수 있지만 사용자가 개발한 제품 또는 프로그램의 일부로 포함하는 경우를 제외하고 다른 사람에게 사용을 허가하거나 배포할 수 없습니다.

Sun RPC 는 사용 또는 판매와 관련하여 설계, 특정 목적에 대한 적합성이나 상업성 여부에 대한 보증을 포함한 어떠한 형태의 명시적 또는 묵시적 보증도 없이 "있는 그대로" 제공됩니다.

Sun Microsystems, Inc.는 Sun RPC 와 관련하여 사용, 수정, 변경 또는 개선을 돕기 위한 어떠한 지원 또는 보증도 제공하지 않습니다.

Sun Microsystems, Inc.는 Sun RPC 및 그 일부분의 저작권, 영업비밀 또는 특허 침해에 대해 어떠한 책임도 지지 않습니다.

Sun Microsystems, Inc.는 어떠한 경우에도 영업 이익 손실 또는 기타 특별, 간접 및 파생적 손해에 대하여 책임을 지지 않습니다. 이는 그러한 손해의 가능성을 사전에 알고 있던 경우에도 마찬가지입니다.

Sun Microsystems, Inc.

2550 Garcia Avenue

Mountain View, California 94043

TINICONV - 1.0.0 라이브러리

카스퍼스키 안티 바이러스 개발 시 Tiniconv – 1.0.0 라이브러리가 사용되었습니다. Copyright (C) Free Software Foundation, Inc. 저작자: Roman Rybalko(http://sourceforge.net/projects/tiniconv/) 사용 허가서: GNU LGPL 2.1(http://www.gnu.org/)

GNU 약소 일반 공중 허가서(Lesser General Public License) v.2.1

전문

대부분의 소프트웨어 라이센스는 소프트웨어를 공유하거나 변경하지 못하게 하는 데 그 목적이 있습니다. 이와는 대조적으로 GNU 일반 공중 허가서(General Public License)는 모든 사용자가 소프트웨어를 자유롭게 사용할 수 있도록 자유 소프트웨어를 공유 및 변경할 수 있는 자유를 보장합니다.

본 약소 일반 공중 허가서(이하 "LGPL")는 자유 소프트웨어 재단(Free Software Foundation)과 이를 채택하기로 결정한 기타 저작자들이 특별히 지정한 일부 소프트웨어 패키지(주로 라이브러리)에 적용됩니다. 누구든지 이

LGPL 을 적용할 수 있지만 해당 상황에서 LGPL 과 GPL 중 어느 것을 선택하는 것이 보다 나은 전략인지 아래 설명을 기준으로 먼저 신중하게 고려해 보는 것이 좋습니다.

자유 소프트웨어라는 말은 무료를 의미하는 것이 아니라 사용이 자유롭다는 것을 의미합니다. 일반 공중 허가서는 자유 소프트웨어를 복제 및 배포하고 원할 경우 이러한 서비스에 대해 비용을 부과할 수 있는 자유와 원할 경우 소스 코드를 받아서 소프트웨어를 변경하거나 소스 코드의 일부를 사용하여 새로운 자유 프로그램을 만들 수 있는 자유를 보장하며 이러한 자유를 인식할 수 있도록 하는 내용을 포함하고 있습니다.

수령인의 권리를 보호하기 위해 배포자들이 수령인의 이러한 권리를 부정하거나 포기하도록 요구하는 행위를 금지해야 합니다. 즉, 라이브러리 복제본을 배포하는 사람이나 수정하는 사람 모두가 지켜야 하는 의무가 있습니다.

예를 들어 유료든 무료든 라이브러리 복제본을 배포할 경우 자신에게 부여된 모든 권리를 수령인에게도 그대로 양도해야 합니다. 또한 소스 코드를 함께 제공하거나 구할 수 있도록 알려주어야 합니다. 또한 라이브러리에 다른 코드를 링크한 경우 링크 코드에 해당하는 개체 파일 전체를 함께 제공하여 수령인이 라이브러리를 수정하고 다시 컴파일한 후 라이브러리에 다시 링크할 수 있도록 해야 합니다. 수령인에게 자신의 권리를 분명히 알 수 있도록 이러한 내용을 보여 주어야 합니다.

자유 소프트웨어 재단은 다음 두 단계를 통해 사용자의 권리를 보호합니다. (1) 라이브러리에 저작권을 설정합니다. (2) LGPL 을 통해 라이브러리를 복제, 배포 또는 수정할 수 있는 권리를 부여합니다.

배포자를 보호하기 위해 자유 라이브러리에 대한 어떠한 보증도 제공하지 않는다는 점을 분명히 밝혀둡니다. 라이브러리가 누군가에 의해 수정되어 재배포되는 경우 최초의 저작자가 만든 원래 버전이 아니라는 점을 분명히 알려야 합니다. 이렇게 할 때 다른 사람에 의해 발생된 문제로 인해 원 저작자의 평판이 실추되는 일을 방지할 수 있습니다.

특허 제도는 자유 소프트웨어의 존재를 끊임없이 위협합니다. 기업이 특허권자로부터 제한적인 사용 허가를 얻어 자유 프로그램 사용자들을 규제할 수 없기를 바랍니다. 따라서 특정 버전의 라이브러리에 대한 어떠한 특허 사용 허가도 LGPL 에 규정된 완전한 자유를 제한하지 않을 것을 요구합니다.

몇몇 라이브러리를 포함한 대부분의 GNU 소프트웨어에는 GPL 이 적용됩니다. 본 LGPL 은 특정 라이브러리에만 적용되며 GPL 과는 상당히 다릅니다. LGPL 은 특정 라이브러리를 자유 소프트웨어가 아닌 프로그램에 링크할 수 있도록 허용하기 위해 사용됩니다.

어떤 프로그램에 라이브러리가 링크되면 정적으로 링크되든지 공유 라이브러리를 사용하든지 간에 둘의 조합은 법적으로 결합 저작물, 즉 원래 라이브러리에서 파생된 저작물로 간주됩니다. 따라서 GPL 은 전체 결합 저작물이 GPL 조건을 만족하는 경우에만 링크를 허용합니다. 그러나 LGPL 은 라이브러리와 다른 코드 간 보다 유연한 링크 조건을 허용합니다.

약소 일반 공중 허가서에서 "약소"는 사용자의 자유를 보호하는 강도가 일반 공중 허가서보다 약하기 때문입니다. 또한 LGPL 은 자유 소프트웨어 개발자들에게 자유 소프트웨어가 아닌 프로그램에 대한 경쟁 우위를 덜 제공합니다. 이러한 이유로 대다수 라이브러리에 GPL 을 사용하고 있습니다. 그러나 LGPL 을 사용하는 것이 유리한 경우가 있습니다.

드문 예이지만 특정 라이브러리를 최대한 광범위하게 사용하도록 장려하여 사실상의 표준으로 만들 필요가 있을 수 있습니다. 이런 경우 자유 소프트웨어가 아닌 프로그램도 해당 라이브러리를 사용할 수 있도록 허용해야 합니다. 이보다 흔한 예로, 자유 라이브러리가 아닌 라이브러리가 광범위하게 사용되며 자유 라이브러리와 동일한 기능을

갖고 있을 수 있습니다. 이 경우 자유 라이브러리를 자유 소프트웨어에만 사용하도록 제한함으로써 얻을 수 있는 유익이 없으므로 LGPL 을 사용합니다.

또 하나의 예는 자유 소프트웨어가 아닌 프로그램에 특정 라이브러리를 사용하도록 허용함으로써 보다 많은 사람들이 자유 소프트웨어를 사용할 수 있게 만드는 경우입니다. 예를 들어 GNU C 라이브러리를 자유 소프트웨어가 아닌 프로그램에 사용할 수 있도록 허용하여 보다 많은 사람들이 GNU 운영 체제와 GNU/Linux 운영 체제를 사용하도록 유도할 수 있습니다.

LGPL 은 사용자의 자유를 보다 약소하게 보호하긴 하지만 라이브러리와 링크된 프로그램의 사용자가 수정된 버전의 라이브러리를 사용하여 프로그램을 실행할 수 있는 자유와 수단을 제공합니다.

복제, 배포 및 수정에 대한 정확한 조건과 규정은 다음과 같습니다. "라이브러리에 기반한 저작물"과 "라이브러리를 사용하는 저작물" 간의 차이에 특별한 주의를 기울여야 합니다. 전자는 라이브러리로부터 파생된 코드를 담고 있는 저작물을 의미하는 반면 후자는 실행을 위해 라이브러리와 결합되어야 하는 저작물을 의미합니다.

복제, 배포 및 수정에 대한 조건과 규정

0. 본 사용 허가 계약은 약소 일반 공중 사용 허가서(이하 "LGPL")에 따라 배포될 수 있다는 고지가 저작권자 또는 기타 관련 권한을 가진 자에 의해 명시된 모든 소프트웨어 라이브러리 또는 기타 프로그램에 적용됩니다. "사용자"는 사용이 허가된 사람을 의미합니다.

"라이브러리"는 프로그램(일부 소프트웨어 함수 및 데이터 사용)과 편리하게 링크되어 실행되도록 소프트웨어 함수와 데이터를 수집해 놓은 것을 의미합니다.

이하 언급되는 "라이브러리"는 본 조건 및 규정에 따라 배포된 모든 소프트웨어 라이브러리 또는 저작물을 의미합니다. "라이브러리에 기반한 저작물"은 라이브러리 또는 저작권법에 따른 모든 2 차적 저작물을 의미합니다. 다시 말해서, 라이브러리의 전부 또는 일부를 그대로 또는 수정하거나 다른 언어로 번역하여 포함한 저작물을 의미합니다. 이후로 다른 언어로의 번역은 별다른 제한 없이 "수정"에 포함하는 것으로 간주합니다.

저작물의 "소스 코드"는 수정하기에 적절한 형식을 의미합니다. 라이브러리에 대한 완전한 소스 코드는 라이브러리에 포함된 모든 모듈의 소스 및 이와 관련된 인터페이스 정의 파일, 그리고 라이브러리의 컴파일과 설치를 제어하는 데 사용된 스크립트를 의미합니다.

LGPL 은 복제, 배포 및 수정 이외의 행위에 대해서는 적용되지 않습니다. 따라서 라이브러리를 사용하는 프로그램을 실행시키는 행위에 대한 제한은 없으며, 이러한 프로그램의 결과물은 작성 도구로 라이브러리를 사용했는지 여부에 관계없이 라이브러리 기반 저작물로 구성된 경우에만 LGPL 이 적용됩니다. 라이브러리 기반 저작물인지 여부는 라이브러리의 역할과 라이브러리를 사용한 프로그램의 역할을 토대로 판단됩니다.

1. 적절한 저작권 표시와 보증 부인 사실을 각 복제물에 명시하는 한, 사용자는 라이브러리의 소스 코드 전체를 받은 그대로 어떠한 매체로든 복제하고 배포할 수 있습니다. 복제 및 배포 시에는 본 사용 허가 계약에 언급된 모든 고지와 보증 부인 사실을 그대로 유지해야 하며 본 사용 허가 계약을 라이브러리 복제본과 함께 배포해야 합니다.

사용자는 배포 시 복제물을 물리적으로 전달하는 비용을 청구할 수 있으며, 원할 경우 유료 보증을 제공할 수 있습니다.

2. 라이브러리 복제본의 전부 또는 일부를 수정할 수 있으며 이를 통해 라이브러리에 기반한 저작물을 창작할 수 있습니다. 또한 수정된 라이브러리 또는 창작된 저작물은 다음 조건을 모두 만족하는 한 위의 제 1 조 규정에 따라 복제 및 배포될 수 있습니다.

a) 수정된 저작물은 소프트웨어 라이브러리여야 합니다.

b) 파일을 수정할 때는 수정한 사실과 수정 날짜를 파일에 명시해야 합니다.

c) 저작물 전체에 대한 사용 권한을 본 사용 허가 계약 조건에 따라 공중에게 무상으로 허용해야 합니다.

d) 수정된 라이브러리에 포함된 기능이 해당 기능을 사용하는 프로그램에서 제공되는 함수 또는 데이터 테이블을 참조하는 경우, 이러한 기능이 호출될 때 전달되는 인수를 제외하고 프로그램이 그러한 함수 또는 테이블을 제공하지 않는 경우에도 기능이 여전히 수행되고 목적하는 모든 부분이 유효하도록 최대의 노력을 기울여야 합니다.

(예를 들면 라이브러리에 포함된 제곱근 계산 함수는 프로그램과 완전히 독립된 목적을 가져야 합니다. 따라서 제 2 조 4 항에 따라 제곱근 계산 함수가 어떠한 프로그램이 제공하는 함수 또는 테이블도 필수적으로 사용하지 않는 형태로 만들어야 합니다. 즉, 프로그램이 제공하지 않더라도 제곱근 계산 함수가 제곱근을 계산해야 합니다.)

위의 조항들은 수정된 저작물 전체에 적용됩니다. 저작물의 특정 부분이 라이브러리에서 파생된 것이 아닌 독립적 저작물로 인정될 만한 이유가 있는 경우 해당 부분을 별도 저작물로 배포할 경우 해당 부분에 본 사용 허가 계약 조항이 적용되지 않습니다. 그러나 해당 부분을 라이브러리에 기반한 저작물의 일부로 함께 배포하는 경우 저작권에 관계없이 저작물 모두의 배포를 본 사용 허가 계약에 의해 관리하고 전체 저작물에 대한 사용 권한을 공중에게 무상으로 부여해야 합니다.

이 규정은 저작자들의 권리를 침해하거나 인정하지 않으려는 것이 아니라 라이브러리에서 파생된 저작물이나 수집 저작물의 배포를 규제하기 위한 것입니다.

라이브러리에서 파생되지 않은 다른 저작물을 라이브러리(또는 라이브러리에 기반한 저작물)와 함께 동일한 저장 또는 배포 매체에 단순히 모아놓은 경우 라이브러리에서 파생되지 않은 다른 저작물에는 본 사용 허가 계약 규정이 적용되지 않습니다.

3. 사용자는 제공받은 라이브러리 복제본에 본 LGPL 대신 GNU GPL 조항을 적용할 수 있습니다. 이렇게 하려면 LGPL 에 대해 언급된 모든 사항을 GNU GPL 버전 2 에 대한 언급으로 대체해야 합니다. (GNU GPL 버전 2 보다 새로운 버전이 나오는 경우 새로운 버전 번호를 지정할 수도 있습니다.) 그 외에 다른 사항은 변경할 수 없습니다.

복제물에 대해 이 변경이 이루어진 후에는 LGPL 로 다시 변경할 수 없으며 이후에 해당 복제물을 기반으로 만들어진 모든 복제물 및 파생 저작물에는 GNU GPL 이 적용됩니다.

이러한 선택 사항은 라이브러리의 코드 일부를 라이브러리가 아닌 일반 프로그램에 복사하려는 경우 유용합니다.

4. 사용자는 제 1 조와 제 2 조의 규정에 따라 라이브러리(또는 제 2 조에 따른 라이브러리의 일부 또는 파생된 저작물)를 목적 코드 또는 실행물 형태로 복제하고 배포할 수 있습니다. 단, 목적 코드 또는 실행물과 상응하는 컴퓨터가 인식할 수 있는 완전한 소스 코드를 제 1 조와 제 2 조 규정에 따라 소프트웨어 교환을 위해 일반적으로 사용되는 매체를 통해 함께 제공해야 합니다.

목적 코드를 지정한 위치로부터 복제할 수 있는 방식으로 배포할 경우, 동일한 위치에서 소스 코드를 복제할 수 있는 동등한 접근 방법을 제공한다면 소스 코드가 목적 코드와 함께 복제되도록 설정되지 않더라도 소스 코드를 배포할 수 있습니다.

5. 라이브러리의 어떠한 부분으로부터의 2 차적 저작물도 포함하지 않지만 컴파일 또는 링크를 통해 라이브러리와 함께 작동하도록 설계된 프로그램은 "라이브러리를 사용하는 저작물"입니다. 이러한 저작물이 별도로 분리되어 있을 때는 라이브러리의 파생 저작물이 아니므로 본 LGPL 이 적용되지 않습니다.

그러나 "라이브러리를 사용하는 저작물"이 라이브러리와 링크되어 생성된 실행물은 라이브러리의 일부를 포함하기 때문에 "라이브러리를 사용하는 저작물"이 아닌 라이브러리의 2 차적 저작물이 됩니다. 따라서 이러한 실행물은 본 LGPL 의 적용을 받습니다. 제 6 조는 이러한 종류의 실행물 배포에 대한 규정입니다.

"라이브러리를 사용하는 저작물"이 라이브러리의 일부인 헤더 파일의 자료를 사용하는 경우 해당 저작물의 소스 코드가 라이브러리의 2 차적 저작물이 아니더라도 목적 코드는 2 차적 저작물이 될 수 있습니다. 이러한 구분의 성립 여부는 그러한 저작물이 라이브러리이거나 라이브러리 없이 링크될 수 있는 경우 매우 중요합니다. 이러한 구분의 판단 기준은 법률적으로 정의되어 있지 않습니다.

이와 같은 개체 파일이 단지 숫자 파라미터와 데이터 구조 레이아웃 및 접근 도구 그리고 10 줄 미만의 작은 인라인 함수와 매크로만 사용하는 경우 법적으로 2 차적 저작물인지에 관계없이 사용이 제한되지 않습니다. (그러나 이러한 목적 코드와 라이브러리의 일부가 포함된 실행물은 여전히 6 조의 적용을 받습니다.)

저작물이 라이브러리의 2 차적 저작물인 경우 해당 저작물의 소스 코드는 제 6 조에 따라 배포할 수 있습니다. 또한 해당 저작물을 포함하는 실행물은 라이브러리에 직접 링크되는지 여부에 관계없이 모두 제 6 조의 적용을 받습니다.

6. 위의 조항들에 대한 한 가지 예외로 라이브러리와 "라이브러리를 사용하는 저작물"을 함께 결합하거나 링크시켜 라이브러리의 일부가 포함된 저작물을 만든 경우 선택한 규정에 따라 배포할 수 있습니다. 이 경우 선택한 규정에는 수령인가 용도에 맞게 저작물을 수정하고 그러한 수정 사항 디버깅을 위해 리버스 엔지니어링이 허용된다는 사항이 포함되어야 합니다.

각 저작물에 라이브러리가 사용되고 있다는 사실과 라이브러리와 라이브러리의 사용에는 본 LGPL 이 적용된다는 사실을 알리는 문구를 모든 복제물에 명시해야 합니다. 또한 본 LGPL 복제본을 함께 제공해야 합니다. 저작물이 실행될 때 저작권이 표시되는 경우 라이브러리에 대한 저작권 표시를 함께 포함해야 하며 LGPL 복제본을 참고할 수 있는 방법을 명시해야 합니다. 또한 다음 중 하나를 만족해야 합니다.

a) 저작물에 대한 모든 수정을 포함하여 라이브러리에 대한 컴퓨터가 인식할 수 있는 완전한 소스 코드를 저작물과 함께 제공해야 합니다. 이 소스 코드는 위 제 1 조 및 제 2 조에 따라 배포해야 합니다. 저작물이 라이브러리와 링크되는 실행물인 경우 사용자가 라이브러리를 수정한 후 링크를 통해 새로운 실행물을 만들 수 있도록 "라이브러리를 사용하는 저작물"로서 컴퓨터가 인식할 수 있는 완전한 목적 코드 또는 소스 코드를 제공해야 합니다. (라이브러리에 포함된 정의 파일의 내용을 변경하는 사용자는 변경한 정의를 사용하게 위해 프로그램을 반드시 다시 컴파일할 필요는 없습니다.)

b) 라이브러리는 적절한 공유 라이브러리 방식을 사용하여 링크되어야 합니다. 적절한 방식이란 (1) 라이브러리의 함수를 실행물 내에 복사하는 것이 아니라 실행 시점에 이미 사용자 컴퓨터 시스템 상에 있는 라이브러리의 복제물을 사용하고 (2) 사용자가 수정된 라이브러리를 설치한 경우에도 수정된 라이브러리가 저작물을 만들 때 사용된 라이브러리 버전과 인터페이스상으로 호환되는 한 적절히 동작해야 합니다.

c) 배포에 필요한 최소 비용만 받고 사용자에게 제 6 조 1 항에 규정된 자료를 배포한다는 3 년 이상 유효한 서면 약정서를 저작물과 함께 제공해야 합니다.

d) 저작물을 지정한 위치에서 복제할 수 있는 방식으로 배포하는 경우 동일한 위치에서 위에 규정된 자료를 복제할 수 있는 동등한 접근 방법을 제공해야 합니다.

e) 사용자가 위에 규정된 자료의 복제물을 이미 받았는지 확인하거나 자신이 사용자에게 이미 복제물을 보냈는지 확인해야 합니다.

실행물이 "라이브러리를 사용하는 저작물"의 형태로 배포되는 경우 실행물을 재생하기 위해 필요한 데이터와 유틸리티 프로그램도 모두 포함되어야 합니다. 그러나 특별한 예외로서 실행물이 실행될 운영 체제의 주요 부분(컴파일러, 커널 등)과 함께 (소스 또는 바이너리 형태로) 배포되는 구성요소는 구성요소 자체가 실행물에 수반되지 않는 한 배포 대상에서 제외되어도 됩니다.

이러한 규정이 일반적으로 운영체제에 수반되지 않는 소유 라이브러리의 사용 허가와 충돌하는 경우 배포하려는 실행물에 본 LGPL 이 적용되는 라이브러리와 소유 라이브러리를 함께 사용할 수 없습니다.

7. 라이브러리에 기반한 저작물로서의 라이브러리의 일부를 본 LGPL 이 적용되지 않는 다른 라이브러리의 일부와 하나의 라이브러리 안에 배치할 수 있습니다. 단, 라이브러리에 기반한 저작물과 그렇지 않은 라이브러리가 별도로 배포될 수 있음을 명시하고 다음 두 가지를 준수해야 합니다.

a) 결합 라이브러리를 구성하는 "라이브러리에 기반한 저작물"의 복제물을 결합되지 않은 독립된 상태로 함께 제공해야 합니다. 이 복제물을 배포할 경우 위의 조항이 적용됩니다.

b) 라이브러리에 기반한 저작물의 일부가 결합 라이브러리에 포함되어 있다는 사실을 명시하고 결합되지 않은 상태의 "라이브러리에 기반한 저작물"의 위치 정보를 알려야 합니다.

8. 본 LGPL 에 의해 명시되지 않은 방법으로 라이브러리를 복제, 수정, 하위 허가, 링크 및 배포할 수 없습니다. 이와 관련된 어떠한 행위도 무효이며 본 LGPL 에 의한 권리가 자동으로 소멸됩니다. 그러나 본 LGPL 의 규정에 따라 라이브러리의 복제물이나 권리를 양도받은 당사자는 본 LGPL 을 준수하는 한 사용 권리가 계속 유지됩니다.

9. 본 LGPL 은 사용자가 서명하지 않기 때문에 반드시 수락할 필요는 없습니다. 그러나 라이브러리나 라이브러리의 2 차적 저작물은 수정 또는 배포하도록 허용하는 것은 본 LGPL 에 의해서만 가능합니다. 본 LGPL 에 동의하지 않을 경우 그러한 수정 또는 배포가 법적으로 금지됩니다. 따라서 라이브러리(또는 라이브러리에 기반한 저작물)을 수정하거나 배포하는 것 자체가 본 LGPL 에 동의한다는 것을 의미하며, 복제, 배포 또는 수정에 관한 모든 조건과 규정도 수락한다는 의미입니다.

10. 라이브러리(또는 라이브러리에 기반한 저작물)가 반복해서 재배포될 때마다 이를 받는 사용자는 본 LGPL 의 규정에 따른 복제, 배포, 링크 또는 수정에 대한 권리를 최초의 사용 허가자로부터 양도받은 것으로 자동으로 간주됩니다. 수령인의 권리 행사를 제한할 수 있는 어떠한 사항도 추가할 수 없습니다. 그러나 또 다른 수령인에게 본 LGPL 을 준수하도록 강제할 책임은 없습니다.

11. 법원 판결 또는 특허권 침해에 대한 주장 또는 특허 문제에 국한되지 않는 기타 이유로 인해 본 LGPL 의 규정에 배치되는 사항이 발생하는 경우에도 그러한 사항이 본 LGPL 의 조건과 규정을 면제하는 것은 아닙니다. 따라서 법원 명령이나 합의 등에 의해 본 LGPL 에 위배되는 사항이 발생한 상황이라도 양측 모두를 만족시킬 수 없다면 라이브러리를 배포할 수 없습니다. 예를 들면 특허 허가가 라이브러리의 복제물을 직간접적으로 양도받은

제 3 자에게 해당 라이브러리를 무상으로 재배포할 수 있게 허용하지 않는다면 그러한 허가와 본 LGPL 을 동시에 만족시키면서 라이브러리를 배포할 수 있는 방법은 없습니다.

본 조항은 특정 상황에서 본 조항의 일부가 유효하지 않거나 적용될 수 없는 경우에도 나머지 부분이 적용됩니다. 따라서 그 이외의 상황에서는 본 조항을 전체적으로 적용하면 됩니다.

본 조항의 목적은 특허 또는 저작권 침해 등을 조장하거나 해당 권리를 인정하지 않으려는 것이 아니라 공중 사용 허가서를 통해 구현된 자유 소프트웨어 배포 체계의 무결성을 보호하기 위한 것입니다. 많은 사람들이 배포 체계를 일관성 있게 적용함으로써 소프트웨어의 다양한 부분에 많은 공헌을 해주었습니다. 소프트웨어를 어떠한 배포 체계를 통해 배포할지 결정하는 것은 저작자와 기증자에게 달려 있으며 사용자가 강요할 수 없습니다.

본 조항은 본 LGPL 의 다른 조항에 따른 결과를 명확하게 설명하기 위한 것입니다.

12. 특허 또는 저작권이 설정된 인터페이스로 인해 특정 국가에서 라이브러리의 배포 또는 사용이 제한되는 경우 본 LGPL 을 라이브러리에 적용한 최초의 저작권자는 문제가 발생하지 않는 국가에 한해 라이브러리를 배포한다는 지역적 제한 조건을 명시적으로 추가할 수 있습니다. 이러한 사항은 본 LGPL 의 일부로 간주됩니다.

13. 자유 소프트웨어 재단은 때때로 본 LGPL 의 개정 버전 또는 새로운 버전을 공표할 수 있습니다. 그러한 새로운 버전은 새로운 문제 또는 현안을 처리하기 위해 세부적인 내용은 차이가 있을 수 있지만 근본 정신은 동일합니다.

각 버전에는 고유한 버전 번호가 부여됩니다. 라이브러리가 특정 버전 번호와 그 이후 버전을 따른다는 사항을 명시하는 경우 해당 버전이나 자유 소프트웨어 재단이 공표한 그 이후 버전을 선택해서 적용해도 되며 버전 번호를 명시하지 않은 라이브러리의 경우 자유 소프트웨어 재단이 공표한 모든 버전 번호의 버전을 적용하면 됩니다.

14. 라이브러리의 일부를 본 LGPL 과 배포 조건이 다른 자유 프로그램과 함께 결합하려는 경우 해당 프로그램 저작자로부터 서면 승인을 받아야 합니다. 자유 소프트웨어 재단이 저작권을 갖는 소프트웨어의 경우 자유 소프트웨어 재단의 승인을 얻어야 합니다. 자유 소프트웨어 재단은 때때로 예외를 두기도 합니다. 자유 소프트웨어 재단은 자유 소프트웨어와 모든 2 차적 저작물을 모두 자유로운 상태로 유지하고 소프트웨어의 공유 및 재사용을 증진하려는 두 가지 목록에 따라 승인 여부를 결정합니다.

보증 없음

15. 본 LGPL 을 따르는 라이브러리는 무상으로 사용이 허가되므로 관련 법률이 허용하는 한도 내에서 어떠한 형태의 보증도 제공되지 않습니다. 라이브러리의 저작권자 또는 배포자가 별도의 서면 보증을 제공하지 않는 한, 특정 목적에 대한 적합성이나 상업성 여부에 대한 보증을 포함한 어떠한 형태의 명시적 또는 묵시적 보증도 없이 "있는 그대로" 이 라이브러리를 배포합니다. 라이브러리의 품질 및 성능과 관련된 모든 위험은 사용자가 부담하며 라이브러리에 결함이 있는 경우 보수 또는 수정에 필요한 모든 경비도 사용자가 부담해야 합니다.

16. 저작권자 또는 배포자가 라이브러리의 손상 가능성을 사전에 알고 있었다 하더라도 발생된 손실이 관련 법규에 의해 보호되고 있거나 별도 서면 보증이 없는 한 저작권자 또는 라이브러리를 원래 상태 또는 수정된 상태로 제공한 배포자는 라이브러리의 사용 또는 비작동으로 인한 손실이나 라이브러리 자체의 손실에 대해 책임지지 않습니다. 이는 사용자나 제 3 자가 라이브러리 조작함으로써 발생한 손실이나 다른 소프트웨어와 라이브러리를 함께 동작함으로써 발생한 데이터 손실 및 부정확한 결과 산출에만 국한되는 것이 아니며 발생된 손실의 일반성 또는 특수성, 원인의 우발성 및 필연성도 전혀 고려되지 않습니다.

조건과 규정 끝

BZIP2/LIBBZIP2 1.0.5 라이브러리

카스퍼스키 안티 바이러스 개발 시 bzip2/libbzip2 1.0.5 라이브러리가 사용되었습니다. Copyright (C) 1996-2007 Julian R Seward. All rights reserved. 사용 조건은 다음과 같습니다.

수정 여부와 상관 없이 소스 및 이진 형식으로 배포하거나 사용하는 것은 다음 조건을 충족할 경우에 한해 허용됩니다.

1. 소스 코드로 배포할 경우 위의 저작권 표시, 본 조건 목록 및 다음 고지 사항을 포함시켜야 합니다.

2. 본 소프트웨어의 원 저작자를 올바르게 알려야 합니다. 원 저작자 이외의 누구도 원래 소프트웨어를 저작했다고 주장해서는 안 됩니다. 본 소프트웨어를 제품에 사용하는 경우 제품 설명서에 원 저작자를 밝히는 것이 의무는 아니지만 바람직합니다.

3. 변경된 소스 버전은 이를 명확하게 표시해야 하며 원래 소프트웨어로 오해되어서는 안 됩니다.

4. 사전 서면 허가 없이는 이 소프트웨어의 2차적 저작물을 추천 또는 홍보하기 위해 저작자의 이름을 사용할 수 없습니다.

본 소프트웨어는 저작자에 의해 "있는 그대로" 제공됩니다. 모든 보증(상품성 및 특정 목적에의 적합성에 대한 묵시적인 보증을 포함하며 이에 제한되지 않음)은 배제됩니다. 저작자는 어떠한 경우에도 본 소프트웨어의 사용과 관련하여 발생한 직접, 간접, 부수적, 특별, 징벌적 또는 파생적 손해(대체 제품 또는 서비스의 조달, 사용할 수 없음, 데이터 손실, 영업 이익 손실 또는 영업 중단으로 인한 손해를 포함하되 이에 제한되지 않음)에 대하여 책임을 지지 않습니다. 이는 계약 위반, 엄격 책임, 잘못(과실 포함)인 경우와 그러한 손해의 가능성을 사전에 알고 있던 경우에도 마찬가지입니다.

Julian Seward, jseward@bzip.org

LIBSPF2-1.2.9 라이브러리

카스퍼스키 안티 바이러스 개발 시 libspf2-2/1/09 라이브러리가 사용되었습니다. Copyright 2005 by Shevek and Wayne Schlitt. All rights reserved, 2 조항 BSD 사용 허가서 조건에 따라 사용

수정 여부와 상관 없이 소스 및 이진 형식으로 배포하거나 사용하는 것은 다음 조건을 충족할 경우에 한해 허용됩니다.

1. 소스 코드로 배포할 경우 위의 저작권 표시, 본 조건 목록 및 다음 고지 사항을 포함시켜야 합니다.

2. 이진 형식으로 배포할 경우 위의 저작권 표시, 본 조건 목록 및 다음 고지 사항을 함께 제공되는 설명서 및/또는 기타 자료에 포함시켜야 합니다.

본 소프트웨어는 저작자에 의해 "있는 그대로" 제공됩니다. 모든 보증(상품성 및 특정 목적에의 적합성에 대한 묵시적인 보증을 포함하며 이에 제한되지 않음)은 배제됩니다. 저작자는 어떠한 경우에도 본 소프트웨어의 사용과 관련하여 발생한 직접, 간접, 부수적, 특별, 징벌적 또는 파생적 손해(대체 제품 또는 서비스의 조달, 사용할 수 없음, 데이터 손실, 영업 이익 손실 또는 영업 중단으로 인한 손해를 포함하되 이에 제한되지 않음)에 대하여 책임을 지지

않습니다. 이는 계약 위반, 엄격 책임, 잘못(과실 포함)인 경우와 그러한 손해의 가능성을 사전에 알고 있던 경우에도 마찬가지입니다.

PROTOCOL BUFFER 라이브러리

카스퍼스키 안티 바이러스 개발 시 Protocol Buffer 라이브러리가 사용되었습니다. Copyright 2008, Google Inc. All rights reserved, 새로운 BSD 사용 허가서 조건에 따라 배포

수정 여부와 상관 없이 소스 및 이진 형식으로 배포하거나 사용하는 것은 다음 조건을 충족할 경우에 한해 허용됩니다.

- 소스 코드로 배포할 경우 위의 저작권 표시, 본 조건 목록 및 다음 고지 사항을 포함시켜야 합니다.
- 이진 형식으로 배포할 경우 위의 저작권 표시, 본 조건 목록 및 다음 고지 사항을 함께 제공되는 설명서 및/또는 기타 자료에 포함시켜야 합니다.
- 사전 서면 허가 없이는 이 소프트웨어의 2 차적 저작물을 추천 또는 홍보하기 위해 Google Inc. 이름 또는 해당 기여자 이름을 사용할 수 없습니다.

본 소프트웨어는 저작권자 및 기여자에 의해 "있는 그대로" 제공됩니다. 모든 보증(상품성 및 특정 목적에의 적합성에 대한 묵시적인 보증을 포함하며 이에 제한되지 않음)은 배제됩니다. 저작권자 또는 기여자는 어떠한 경우에도 본 소프트웨어의 사용과 관련하여 발생한 직접, 간접, 부수적, 특별, 징벌적 또는 파생적 손해(대체 제품 또는 서비스의 조달, 사용할 수 없음, 데이터 손실, 영업 이익 손실 또는 영업 중단으로 인한 손해를 포함하되 이에 제한되지 않음)에 대하여 책임을 지지 않습니다. 이는 계약 위반, 엄격 책임, 잘못(과실 포함)인 경우와 그러한 손해의 가능성을 사전에 알고 있던 경우에도 마찬가지입니다.

Protocol Buffer 컴파일러에서 생성되는 코드는 생성 시 사용된 입력 파일 소유자가 소유합니다. 본 코드는 독립 실행형이 아니며 링크를 위한 지원 라이브러리가 필요합니다. 이 지원 라이브러리에는 위의 사용 허가서가 적용됩니다.

용어집

사용자가 신뢰하는 컨텐츠에 대한 웹 리소스의 마스크 및 주소 목록입니다. 악성 개체가 존재할 수 있으므로 카스퍼스키 랩 프로그램은 목록 항목 중 일부에 해당하는 웹 페이지는 검사하지 않습니다.

프로그램 활성화

프로그램 활성화 절차는 활성화 코드 입력 및 키 얻기로 구성되며 이러한 절차를 통해 프로그램에서는 해당 사용자에게 프로그램을 사용할 권한이 있는지 결정하고 라이센스 만료일을 확인할 수 있습니다.

사용 중인 라이센스

카스퍼스키 랩 프로그램을 작동하는 데 현재 사용되는 라이센스입니다. 이 라이센스를 통해 전체 기능의 만료일 및 프로그램의 라이센스 정책이 정의됩니다. 한 프로그램당 사용 중 상태인 라이센스는 하나뿐입니다.

추가 라이센스

카스퍼스키 랩 프로그램의 작동을 위해 추가되었지만 활성화되지 않은 라이센스입니다. 사용 중인 라이센스가 만료되면 추가 라이센스가 유효 상태가 됩니다.

관리 서버 인증서

관리 콘솔을 연결하거나 사용자의 컴퓨터와 데이터를 교환할 때 관리 서버를 인증할 수 있는 인증서입니다. 관리 서버 인증서는 관리 서버를 설치할 때 만들어지며 프로그램 설치 폴더에 있는 **Cert** 하위 폴더에 저장됩니다.

대체 NTFS 스트림

NTFS 데이터 스트림(대체 데이터 스트림)은 추가 속성 또는 파일 정보를 포함할 수 있도록 만들어진 스트림입니다.

NTFS 파일 시스템의 각 파일은 스트림의 집합입니다. 이 중 하나는 파일을 연 후에 볼 수 있는 파일 컨텐츠를 포함하고 있고 다른 스트림(대체 스트림)은 메타 데이터를 포함하며, HFS(Hierarchical File System)라고 불리는 Macintosh 의 기존 파일 시스템과 같은 다른 시스템과 NTFS 가 호환되도록 만들어졌습니다. 스트림은 만들거나 삭제하거나 따로 보관하거나 이름을 바꿀 수 있으며 프로세스로 실행할 수도 있습니다.

대체 스트림은 침입자가 데이터를 몰래 전송하거나 컴퓨터에서 훔치는 데 사용할 수도 있습니다.

프로그램 모듈

카스퍼스키 랩 설치 패키지에 포함된 파일로 주요 작업 수행을 담당합니다. 특정 실행 모듈은 프로그램에서 수행하는 작업(실시간 감시, 수동 검사, 업데이트)의 각 유형과 일치합니다. 메인 창에서 컴퓨터 전체 검사를 실행하면 이 작업의 모듈 실행이 시작됩니다.

프로그램 설정

모든 작업 유형에 공통적으로 적용되는 프로그램 설정으로 프로그램 성능 설정, 보고서 설정, 백업 저장소 설정 등 프로그램의 작동을 전체적으로 통제합니다.

압축 파일

개체를 하나 이상 "포함"하는 파일로서, 이러한 개체 역시 압축 파일일 수 있습니다.

사용 가능한 업데이트

일정 기간 동안 누적된 중요 업데이트 및 프로그램의 아키텍처에 대한 변경 사항을 비롯하여 카스퍼스키 랩 프로그램 모듈에 대한 업데이트 집합입니다.

백업 복사본

예를 들어 업데이트된 데이터베이스에서 검사하는 경우와 같이 나중에 파일을 복구할 때를 대비하여 파일을 처리하기 전에 백업 복사본을 만들어 백업 저장소 영역에 보관합니다.

백업 저장소

첫 번째로 치료되거나 삭제되기 전에 만든 개체의 백업 복사본을 저장하기 위해 특별히 만들어진 저장소입니다.

피싱 웹 주소 목록

카스퍼스키 랩 전문가가 피싱으로 정의한 웹사이트의 목록입니다. 이 목록은 정기적으로 업데이트되어 카스퍼스키 랩 프로그램에 포함됩니다.

의심스러운 웹 주소 목록

잠재적으로 위험한 것으로 간주되는 콘텐츠를 포함하는 웹사이트의 목록입니다. 이 목록은 카스퍼스키 랩 전문가에 의해 작성되었으며 정기적으로 업데이트되어 카스퍼스키 랩 프로그램 패키지에 포함됩니다.

블랙리스트 파일

소유자가 라이센스 동의서를 위반하여 블랙리스트에 포함된 카스퍼스키 파일의 정보 및 발행되었지만 어떤 이유로 인해 판매되지 않거나 교체된 파일의 정보를 포함하는 데이터베이스입니다. 블랙리스트 파일은 카스퍼스키 랩 프로그램의 작동에 필요한 요소이며 파일 컨텐츠는 데이터베이스와 함께 업데이트됩니다.

개체 차단

외부 프로그램의 개체에 대한 액세스를 차단하는 것입니다. 차단된 개체에서는 읽기, 실행, 변경 또는 삭제 작업을 수행할 수 없습니다.

부트 바이러스

컴퓨터 하드 드라이브의 부트 섹터를 감염시키는 바이러스입니다. 이 바이러스는 시스템이 재부팅되는 동안 메모리로 바이러스를 로드하며 원래의 부트 로더 코드 대신 바이러스 코드에게 통제 권한을 전달합니다.

압축 파일

압축 해제 프로그램 및 실행을 위한 운영 체제 지침이 포함된 압축 파일입니다.

위험 개체

바이러스를 포함하는 개체로, 이러한 개체에 액세스하면 컴퓨터가 감염될 수 있으므로 액세스하지 않는 것이 좋습니다. 감염된 개체가 탐지되면 카스퍼스키 랩 프로그램 중 하나를 사용하여 치료하거나 치료할 수 없는 경우에는 삭제해야 합니다.

데이터베이스 업데이트

항상 최신 상태를 유지하기 위해 카스퍼스키 랩 프로그램에서 수행하는 기능 중 하나입니다. 업데이트 과정 중에 데이터베이스가 카스퍼스키 랩 업데이트 서버에서 컴퓨터로 다운로드되어 자동으로 프로그램과 연결됩니다.

데이터베이스

카스퍼스키 랩 전문가가 제작한 데이터베이스로 현재 존재하는 모든 컴퓨터 보안위협과 탐지 및 치료 방법에 대한 상세한 설명이 포함되어 있습니다. 카스퍼스키 랩은 새로운 보안위협이 나타날 때마다 이러한 데이터베이스를 지속적으로 업데이트합니다. 보안위협 탐지 성능을 더 높이려면 카스퍼스키 랩의 업데이트 서버에서 데이터베이스를 정기적으로 복사할 것을 권장합니다.

개체 삭제

원래 위치(하드 드라이브, 폴더, 네트워크 리소스)에서 물리적으로 삭제하는 개체 처리 방법입니다. 이 방법은 어떠한 이유로든 치료할 수 없는 위험 개체에 적용할 것을 권장합니다.

다시 시작할 때 개체 치료

치료하는 당시에 다른 프로그램에서 사용 중인 감염된 개체를 처리하는 방법입니다. 감염된 개체의 복사본을 만들어 치료한 다음 시스템이 다시 시작한 후에 치료된 개체가 감염된 원본 개체를 대체하는 방식으로 구성됩니다.

디스크 부트 섹터

부트 섹터는 컴퓨터의 하드 드라이브, 플로피 또는 기타 데이터 저장소 장치에 있는 특정 영역으로 디스크의 파일 시스템에 있는 정보와 운영 체제를 시작하는 부트 로더 프로그램이 포함되어 있습니다.

부트 섹터를 감염시키는 바이러스를 부트 바이러스라고 합니다. 카스퍼스키 랩 프로그램에서는 부트 섹터에 대해 바이러스 검사를 수행하고 감염이 발견되면 이를 치료합니다.

도메인 이름 서비스 (DNS)

호스트(컴퓨터 또는 기타 네트워크 장치)의 이름을 IP 주소로 변환하기 위해 분산된 시스템으로 TCP/IP 네트워크에서 작동합니다. 또한 IP 주소(PTR 레코드)에 따라 호스트의 이름을 결정하여 역방향 요청도 저장 및 처리할 수 있습니다. DNS 이름은 사용자가 아니라 항상 네트워크 프로그램에서 확인합니다.

이중 홈 게이트웨이

네트워크 간에 데이터를 전송하는 2 개의 네트워크 어댑터(각기 다른 네트워크에 연결)가 포함된 컴퓨터입니다.

이벤트 심각도 레벨

카스퍼스키 랩 프로그램이 작동하는 중에 기록된 이벤트에 대한 설명으로 다음과 같은 4 가지 레벨로 나눠집니다.

- **매우 중요한 이벤트**
- **기능 실패**
- **경고**
- **정보 메시지**

동일한 유형의 이벤트도 발생 상황에 따라 심각도 레벨이 다를 수 있습니다.

제외

제외는 카스퍼스키 랩 프로그램에서 수행하는 검사로부터 제외된 개체입니다. 특정 형식의 파일은 검사에서 제외하거나 파일 마스크를 사용하거나 진단 명 분류에 따라 보안위협 형태별로 특정 영역(예: 폴더, 프로그램), 프로그램 프로세스 또는 개체를 제외할 수 있습니다. 제외 집합별로 작업이 할당될 수 있습니다.

파일 마스크

와일드카드를 사용하여 파일 이름 및 확장자를 나타낸 것입니다. 파일 마스크에는 * 및 ? 등 2 개의 표준 와일드카드가 사용됩니다. *는 무한한 문자를 나타내고 ?는 단일 문자를 나타냅니다. 이러한 와일드카드를 사용하여 어떤 파일이든 표시할 수 있습니다. 이름과 확장자는 항상 마침표로 구분됩니다.

하드웨어 포트

케이블이나 플러그가 연결될 수 있는 컴퓨터 하드웨어 구성요소의 소켓(LPT 포트, 직렬 포트, USB 포트)입니다.

헤더

메시지 또는 파일의 시작 부분에 나타나는 정보로 파일(또는 메시지) 상태 및 처리에 대한 낮은 수준의 데이터로 구성되어 있습니다. 특히 이메일 메시지 헤더에는 발신자/수신자 및 날짜 정보와 같은 데이터가 포함되어 있습니다.

휴리스틱 분석기

안티 바이러스 데이터베이스로 탐지할 수 없는 보안위협에 대한 탐지 기술입니다. 이 기술을 사용하면 알려지지 않는 바이러스 또는 알려진 바이러스의 새로운 변형으로 인한 감염이 의심되는 개체를 탐지할 수 있습니다.

휴리스틱 분석기를 사용하면 보안위협을 최대 92%까지 탐지할 수 있습니다. 이 메커니즘은 상당히 효과적이며 정상적인 개체를 탐지하는 일은 거의 없습니다.

휴리스틱 분석기로 탐지된 파일은 감염이 의심됩니다.

ICHECKER 기술

iChecker 는 검사 설정(안티 바이러스 데이터베이스 및 설정)이 변경되지 않은 경우 마지막 검사 이후로 변경되지 않은 개체를 제외하여 바이러스 검사의 속도를 증가시키는 기술입니다. 각 파일의 정보는 특수 데이터베이스에 저장됩니다. 이 기술은 실시간 감시 및 수동 검사 모드에 사용됩니다.

예를 들어 카스퍼스키 랩 프로그램에서 검사하여 감염되지 않음 상태가 할당된 압축 파일이 있다고 가정합니다. 이 압축 파일이 바뀌거나 검사 설정이 변경되지 않은 경우 프로그램은 다음 번에 이 압축 파일을 건너뜁니다. 그러나 압축 파일에 새로운 컨텐츠를 추가하여 압축 파일이 변경된 경우, 검사 설정을 변경하거나 안티 바이러스 데이터베이스를 업데이트한 경우 해당 압축 파일은 다시 검사됩니다.

iChecker 기술에는 다음과 같은 몇 가지 제한이 있습니다.

- 파일이 마지막 검사 후에 수정되었는지 확인하는 것보다 파일을 검사하는 속도가 더 빠르기 때문에 이 기술은 대용량 파일에서는 작동하지 않습니다.
- 이 기술이 지원하는 형식의 수가 제한되어 있습니다(exe, dll, lnk, ttf, inf, sys, com, chm, zip, rar).

호환되지 않는 프로그램

타사 개발자가 만든 안티 바이러스 프로그램 또는 카스퍼스키 Administration Kit 를 통한 관리를 지원하지 않는 카스퍼스키 랩 프로그램입니다.

감염된 개체

악성 코드를 포함하고 있는 개체입니다. 개체 코드의 일부와 알려진 보안위협 코드의 일부가 완전히 일치하는 경우 탐지됩니다. 해당 개체는 컴퓨터를 감염시킬 수 있으므로 사용하지 말 것을 권장합니다.

입력/출력 포트

하드웨어 구성요소와 데이터를 교환하기 위한 프로세서(예: Intel)의 서버입니다. 입력/출력 포트는 특정 하드웨어 구성요소와 연결되어 있으며 프로그램에서 포트를 지정하여 데이터를 교환할 수 있습니다.

시작 시나리오로 설치

카스퍼스키 랩 프로그램의 원격 설치 방법으로 원격 설치 작업의 시작을 개별 사용자 계정 또는 여러 사용자 계정에 할당할 수 있습니다. 도메인에 사용자를 등록하면 해당 사용자가 등록된 클라이언트 컴퓨터에서 프로그램 설치가 시작됩니다. 이 방법은 Microsoft Windows 98/Me 운영 체제를 실행하는 컴퓨터에서 프로그램을 설치할 경우 권장됩니다.

인터셉터

특정 유형의 이메일을 검사하는 프로그램의 하위 구성요소입니다. 설치에 적용되는 인터셉터의 집합은 프로그램에서 배포하는 역할 또는 역할의 조합에 따라 달라집니다.

인터넷 프로토콜(IP)

1974 년에 개발된 후로 변경되지 않고 사용된 인터넷의 기본 프로토콜로 컴퓨터 간의 데이터를 전송할 때 기본적인 작업을 수행하며 TCP 및 UDP 와 같은 높은 수준의 프로토콜에 대한 토대가 됩니다. IP 는 연결 및 오류 처리를 관리합니다. NAT 및 마스크와 같은 기술을 통해 적은 수의 IP 주소를 사용하는 다수의 개인 네트워크를 숨길 수 있으므로 상대적으로 제한되는 IPv4 주소 공간을 사용하여 지속적으로 증가하는 인터넷에 대한 요구 사항을 충족할 수 있습니다.

카스퍼스키 랩 업데이트 서버

프로그램에서 데이터베이스 및 모듈 업데이트를 다운로드하는 카스퍼스키 HTTP 및 FTP 서버의 목록입니다.

라이센스 키 파일

확장자가 **.key** 인 파일로 개인적인 "라이센스 키"를 의미하며 카스퍼스키 랩 프로그램 작동에 필요한 파일입니다. 라이센스 키 파일은 카스퍼스키 랩 판매처를 통해 구입한 경우 제품에 포함되어 있으며 온라인으로 구입한 경우 이메일로 전송됩니다.

라이센스 유효 기간

카스퍼스키 랩 프로그램의 모든 기능을 사용할 수 있는 기간입니다. 일반적으로 라이센스 유효 기간은 설치 날짜로부터 1 년간 지속됩니다. 라이센스가 만료된 후에는 프로그램에서 사용할 수 있는 기능이 감소하며 프로그램 데이터베이스를 업데이트할 수 없습니다.

허락한 웹 주소 목록

카스퍼스키 랩 프로그램에서 액세스를 차단하지 않은 웹 리소스의 마스크 및 주소 목록입니다. 이 주소 목록은 프로그램 설치 구성 중에 사용자가 직접 작성합니다.

허락한 이메일 목록

(화이트 리스트와 동일한 개념)

메시지를 보내는 이메일 주소 중 카스퍼스키 랩 프로그램에서 검사하지 않아도 되는 이메일 주소의 목록입니다.

차단한 이메일 목록

(블랙 리스트와 동일한 개념)

메시지를 보내는 이메일 주소 중 컨텐츠에 관계없이 카스퍼스키 랩 프로그램에서 차단해야 하는 이메일 주소의 목록입니다.

차단한 웹 주소 목록

카스퍼스키 랩 프로그램에서 액세스를 차단한 웹 리소스의 마스크 및 주소 목록입니다. 이 주소 목록은 프로그램 설치 구성 중에 사용자가 직접 작성합니다.

감시할 웹 주소 목록

카스퍼스키 랩 프로그램에서 필수적으로 악성 개체를 검사해야 하는 웹 리소스의 마스크 및 주소 목록입니다.

메일 데이터베이스

특정 형식의 이메일을 포함한 데이터베이스로 컴퓨터에 저장됩니다. 모든 수신/발신 이메일은 해당 메일이 수신/발송된 후에 메일 데이터베이스에 보관되며 이러한 데이터베이스는 컴퓨터 전체 검사를 수행하는 동안 검사됩니다.

실시간 감시가 활성화되어 있는 경우 각 이메일은 수신 및 발송되는 순간에 실시간으로 바이러스 분석이 실시됩니다.

메시지 삭제

스팸 신호가 포함된 이메일 메시지를 실제로 제거하여 처리하는 방법입니다. 이 방법은 스팸이 확실한 메시지에 대해 사용하는 것이 좋습니다. 백업 옵션이 활성화되어 있는 경우 메시지를 삭제하기 전에 해당 메시지의 복사본을 백업에 저장합니다.

감시하는 개체

방화벽을 통과하여 HTTP, FTP 또는 SMTP 프로토콜을 통해 전송되어 카스퍼스키 랩 프로그램에 검사를 위해 전달되는 개체입니다.

격리 저장소로 개체 이동

파일에 대한 액세스를 차단하고 원래 위치에서 격리 저장소 폴더로 파일을 이동하여 감염 위험 개체를 처리하는 방법입니다. 격리 저장소에서는 개체가 암호화된 형태로 저장되므로 감염의 위협이 제거됩니다.

네트워크 포트

네트워크를 통해 호스트로 전송되는 IP 형식 데이터 패킷의 대상 주소를 결정하고 단일 호스트에서 실행되는 다양한 프로그램이 서로 개별적으로 데이터를 받을 수 있도록 하는 TCP 및 UDP 파라미터입니다. 각 프로그램은 특정 포트를 통해 받은 데이터를 처리합니다. 이를 해당 포트를 프로그램에서 "수신"한다고도 합니다.

몇몇 일반 네트워크 프로토콜의 경우 항상 사용하는 표준 포트 번호가 있습니다. 예를 들어 웹 서버는 항상 TCP 포트 80 에서 HTTP 요청을 받습니다. 그러나 일반적으로 프로그램에서는 종류를 막론하고 모든 포트와 프로토콜을 사용할 수 있습니다. 사용 가능한 값은 1 ~ 65535 입니다.

알림 템플릿

검사에서 감염 개체가 탐지되었다는 알림을 생성할 기본 템플릿입니다. 알림 템플릿에는 알림 모드, 전송 방식 및 보낼 메시지의 텍스트 등을 지정하는 설정 조합이 포함되어 있습니다.

감염 위험 개체

알려진 바이러스의 변형된 코드 또는 바이러스 코드와 유사한 코드를 포함하지만 아직까지 카스퍼스키 랩에 알려지지 않은 개체입니다. 잠재적으로 감염 위험이 있는 파일은 휴리스틱 분석기로 탐지됩니다.

초기화

격리 저장소 또는 백업에 있는 원본 개체를 격리 저장소 또는 사용자가 지정한 다른 폴더로 이동하거나 치료 또는 삭제하기 전에 원래 발견된 폴더로 개체를 이동하는 작업입니다.

개체 치료

감염된 개체의 처리 방법으로 데이터의 전부 또는 일부를 복구하거나 개체를 치료할 수 없다고 결정을 내립니다. 개체 치료는 데이터베이스 레코드를 사용하여 수행됩니다. 치료 도중 데이터의 일부가 손실될 수 있습니다.

음란 메시지

저속한 언어를 포함하는 이메일 메시지입니다.

OLE 개체

첨부된 개체 또는 다른 파일에 포함된 개체입니다. 카스퍼스키 랩 프로그램은 OLE 개체에 대해 바이러스 검사를 수행합니다. 예를 들어, Microsoft Office Excel 표를 Microsoft Office Word 문서에 삽입할 경우 표는 OLE 개체로 검사됩니다.

감염될 가능성이 있는 개체

구조 또는 형식상의 이유로 침입자가 악성 개체를 저장하고 분포할 "컨테이너"로 사용할 수 있는 개체입니다. 이러한 파일은 대개 확장자가 .com, .exe, .dll 등인 실행 파일입니다. 이러한 파일의 악성 코드는 활성화될 위험이 매우 높습니다.

감시 상태

컴퓨터 보안의 정도를 간략하게 나타내는 감시의 현재 상태입니다.

프로토콜

클라이언트와 서버 간 상호 작용을 통제하도록 명확하게 정의되고 표준화된 규칙의 집합입니다. 널리 알려진 프로토콜과 관련된 서비스에는 HTTP(WWW), FTP 및 NNTP(뉴스) 등이 있습니다.

프록시 서버

사용자가 다른 네트워크 서비스에 간접 요청을 할 수 있도록 하는 컴퓨터 네트워크 서비스입니다. 먼저 사용자가 프록시 서버에 접속하고 다른 서버에 있는 리소스(예: 파일)를 요청합니다. 그러면 프록시 서버에서 지정된 서버에 접속하여 해당 리소스를 가져오거나 프록시에 자체 캐시가 있는 경우 해당 서버의 캐시에서 리소스를 반환합니다. 경우에 따라 특정 이유로 프록시 서버에서 사용자의 요청 또는 서버의 응답을 수정하기도 합니다.

격리 저장소

검사 동안 또는 실시간 감시를 통해 탐지된 모든 감염 개체가 위치하고 있는 특정 폴더입니다.

실시간 감시

개체가 실시간으로 악성 코드에 대한 검사를 받는 프로그램의 작동 모드입니다.

프로그램에서는 개체를 열고자 하는 모든 시도(읽기, 쓰기 또는 실행)를 가로채어 보안위협 검사를 수행합니다. 감염되지 않은 개체는 사용자에게 전달되고 보안위협 또는 보안위협을 포함하고 있는 것으로 의심되는 개체는 작업 설정에 따라 치료, 삭제 또는 격리되는 방식으로 처리됩니다.

권장 레벨

컴퓨터에 대한 최적의 감시 레벨을 제공하기 위해 프로그램 설정을 기준으로 카스퍼스키 랩 전문가가 권장하는 보안의 레벨입니다. 이 레벨은 기본적으로 사용하도록 설정되어 있습니다.

스크립트

일반적으로 소규모 특정 작업을 실행하도록 작성된 컴퓨터 프로그램 또는 프로그램(기능)의 개별 부분으로 대개 하이퍼텍스트에 포함된 프로그램에 사용됩니다. 예를 들어 특정 웹사이트를 열 때 스크립트가 실행됩니다.

실시간 감시가 활성화되어 있는 경우 프로그램에서는 스크립트의 실행을 추적하고 가로채어 바이러스 검사를 수행합니다. 검사 결과에 따라 스크립트의 실행을 차단하거나 허용할 수 있습니다.

보안 레벨

보안 레벨은 사전 설정된 구성요소 구성으로 정의됩니다.

SOCKS

내부 및 외부 네트워크에서 컴퓨터간 점 대 점 연결을 설정하는 프록시 서버 프로토콜입니다.

자동 시작 개체

컴퓨터에 설치된 운영 체제 및 소프트웨어를 시작하고 정확하게 작동시켜야 하는 프로그램의 집합입니다. 이러한 개체는 운영 체제가 시작할 때마다 실행됩니다. 이러한 개체에 감염되어 운영 체제에 대한 액세스를 차단할 수도 있는 바이러스도 있습니다.

의심스러운 개체

알려진 바이러스의 변형된 코드 또는 바이러스 코드와 유사한 코드를 포함하지만 아직까지 카스퍼스키 랩에 알려지지 않은 개체입니다. 감염의심 개체는 휴리스틱 분석기를 통해 탐지됩니다.

작업

카스퍼스키 랩 프로그램에서 수행하는 기능은 **실시간 파일 감시, 컴퓨터 전체 검사, 데이터베이스 업데이트** 등의 작업으로 구현됩니다.

작업 설정

각 작업 유형별로 적용되는 프로그램 설정입니다.

트래픽 검사

모든 프로토콜(예: HTTP, FTP 등)을 통해 전송된 개체에 대한 최신 버전 데이터베이스의 정보를 사용하는 실시간 검사입니다.

신뢰하는 프로세스

실시간 감시 모드에서 카스퍼스키 랩 프로그램이 파일 작업을 모니터링하지 않는 프로그램의 프로세스입니다. 즉, 신뢰하는 프로세스에서 실행하거나 열거나 저장하는 개체는 검사를 받지 않습니다.

알려지지 않은 바이러스

데이터베이스에 저장된 정보가 전혀 없는 새로운 바이러스입니다. 일반적으로 알려지지 않은 바이러스는 휴리스틱 분석기를 통해 프로그램에서 발견하며 탐지된 개체는 감염 위험으로 분류됩니다.

업데이트

카스퍼스키 랩 업데이트 서버에서 검색된 새로운 파일(데이터베이스 또는 프로그램 모듈)을 대체/추가하는 절차입니다.

업데이트 패키지

소프트웨어 업데이트를 위한 파일 패키지로 인터넷에서 다운로드되어 컴퓨터에 설치됩니다.

긴급 업데이트

카스퍼스키 랩 프로그램 모듈에 대한 중요 업데이트입니다.

바이러스 활동 임계값

한정된 기간 내에 특정 유형의 이벤트에 대해 허용 가능한 최대 레벨입니다. 이를 초과할 경우 과도한 바이러스 활동 및 바이러스 급증의 위협으로 간주됩니다. 이 기능은 바이러스가 급증하는 동안 매우 중요한 역할을 하며 이 기능을 통해 관리자가 바이러스 급증의 위협에 대해 시의적절하게 대처할 수 있습니다.

바이러스 급증

컴퓨터를 바이러스로 감염시키고자 연속적으로 발생하는 고의적 시도입니다.

바이러스 급증 카운터

바이러스 급증 알림을 생성할 기본 템플릿입니다. 바이러스 급증 카운터에는 바이러스 활동 임계값, 전송 방식 및 보낼 메시지의 텍스트 등을 지정하는 설정 조합이 포함되어 있습니다.

카스퍼스키 랩

1997 년에 설립된 카스퍼스키 랩은 정보 보안 기술에 분야에 잘 알려진 리더가 되었습니다. 다양한 데이터 보안 소프트웨어를 생산하며 높은 수준의 안티 바이러스, 안티 스팸 그리고 안티 해킹 시스템을 제공합니다.

카스퍼스키 랩은 국제적인 회사입니다. 러시아에 본부가 있으며 영국, 프랑스, 독일, 일본, 베네룩스 국가, 중국, 폴란드, 루마니아, 한국, 그리고 미국에 지부가 있습니다. 최근에 프랑스에 새로운 유럽 안티 바이러스 센터 지부가 설립되었습니다. 카스퍼스키 랩의 파트너 네트워크는 세계의 500 여개의 회사를 포함합니다.

오늘날 카스퍼스키 랩은 10 명의 MBA 소지자, 16 명의 PhD 소지자를 포함한 천명이 넘는 전문가를 고용하고 있습니다. 카스퍼스키 랩의 최상급 안티 바이러스 전문가들은 모두 컴퓨터 안티 바이러스 연구 협회(CARO)의 멤버입니다.

회사의 가장 중요한 자산은 14 년동안 전문가들이 끊임없이 컴퓨터 바이러스와 싸우며 쌓은 특별한 지식과 경험입니다. 컴퓨터 바이러스 행동에 관한 자세한 분석은 저희 전문가들이 악성 프로그램이 어떻게 개발될지 예측하고 새로운 유형의 공격에 대해 신속한 보안을 제공하는 것이 가능하게 합니다. 미래에 일어날 공격에 저항하는 것이 카스퍼스키 랩 제품의 기본 방침입니다. 항시 저희 회사의 제품은 고객들에게 다른 회사에 비해 한걸음 앞선 안티 바이러스 보안을 제공합니다.

몇 년에 걸친 노력은 저희 회사를 최고의 안티 바이러스 소프트웨어 개발사중 하나로 만들었습니다. 카스퍼스키 랩은 안티 바이러스 보안에 관하여 가장 높은 기준을 개발한 첫번째 회사입니다. 본 사의 대표적 제품 카스퍼스키 안티 바이러스는 모든 수준의 네트워크 워크스테이션, 파일 서버, 메일 시스템, 방화벽, 인터넷 게이트웨이, 포켓용 컴퓨터에 보안을 제공합니다. 편리하고 사용하기 쉬운 관리 도구는 컴퓨터와 기업 네트워크에 최대한 자동화된 안티 바이러스 보안을 제공합니다. 많은 알려진 생산자는 카스퍼스키 안티 바이러스 커널을 사용합니다. 이러한 생산자는 Nokia ICG(미국), F-Secure(핀란드), Aladdin(이스라엘), Sybari(미국), G Data(독일), Deerfield(미국), Alt-N(미국), Microworld(인도), 그리고 BorderWare(캐나다)를 포함합니다.

카스퍼스키 랩의 고객은 본사 제품의 안정적인 운영과 각각의 사업 기준에 맞는 대응을 보증하는 다양한 추가 서비스로부터 이득을 얻고 있습니다. 저희는 기업 안티 바이러스 체제를 디자인, 적용, 지원합니다. 카스퍼스키 랩의 안티 바이러스 데이터베이서는 매 시간 업데이트 됩니다. 본사는 소비자에게 24 시간 기술 지원 서비스를 여러 언어로 제공하고 있습니다.

질문, 의견, 혹은 제안이 있다면 판매처나 카스퍼스키 랩에 직접 연락하실 수 있습니다. 저희 제품과 관련된 모든 것에 있어서 전화나 이메일을 통해 여러분을 도울 것입니다. 여러분의 모든 질문 사항에 대해 자세하고 포괄적인 답변을 해드릴 것입니다.

카스퍼스키 랩 공식 사이트:	http://www.kaspersky.co.kr
바이러스 백과사전:	http://www.viruslist.com
안티 바이러스 연구소:	newvirus@kaspersky.co.kr (의심스러운 개체는 반드시 압축해서 보내주십시오.)
카스퍼스키 랩 웹 포럼:	http://www.kaspersky.co.kr/forum_login.html

카스퍼스키 랩 최종 사용자 라이센스 계약

모든 사용자 공지 사항: 이 제품을 사용하기 전에 이하의 법적 계약 내용을 주의 깊게 읽어 보시기 바랍니다.

라이센스 계약 창에서 동의 버튼을 클릭하면 본 계약의 이용약관을 승낙함을 의미합니다. **본 조작은 본 계약에 동의하고 본 계약의 당사자임을 서명함을 뜻하며 본 계약은 귀하가 사인한 서면 계약과 동등한 효력을 같고 있음을 승인합니다.** 만약 본 계약의 이용약관에 동의하지 않으시면 소프트웨어의 설치를 취소하여 소프트웨어를 설치하지 마시기 바랍니다.

라이센스 계약 창에서 동의 버튼을 클릭한 후 본 계약의 이용약관에 따라 소프트웨어를 사용할 수 있는 권리를 갖게 됩니다.

1. 정의

1.1. **소프트웨어**는 소프트웨어, 사용 설명서, 상관 해석 혹은 기타 자료를 뜻하며 임의의 업데이트도 포함합니다.

1.2. **권리 소유자**(독점 혹은 기타를 물론하고 소프트웨어에 대한 모든 권리 소유자)는 러시아 연방 법률에 의하여 성립된 Kaspersky Lab ZAO 회사입니다.

1.3. **컴퓨터**는 소프트웨어를 설치할 개인용 컴퓨터, 랩톱, 워크스테이션, 개인용 디지털 어시스턴트,"스마트 폰", 핸드 헬드 장치, 혹은 기타 전자 장치(본 장치를 위해 소프트웨어를 디자인)을 포함한 하드웨어를 뜻합니다.

1.4. **최종 사용자(귀하/귀하의)**는 자신을 대표하여 소프트웨어를 설치 및 사용하거나 소프크웨어의 사본을 합법적으로 사용하는 개인을 뜻합니다. 혹은 고용주등과 같은 조직을 대표하여 소프트웨어를 다운로드 혹은 설치할 경우, *"귀하"* 는 더 나아가 소프트웨어를 다운로드 혹은 설치한 조직을 뜻하며 또한 본 조직은 그를 대표하여 본 계약을 승낙하는 사람에게 권리를 부여함을 임의합니다. 속어 *"조직"* 은 임의의 조합, 유한책임회사, 회사, 협회, 주식회사, 신탁회사, 합작회사, 노동기구, 법인격 없는 조직, 혹은 정부 당국 등을 포함하지만 이에 한하지 않습니다.

1.5. **파트너**는 권리 소유자와의 계약 및 라이센스에 근거하여 소프트웨어를 배분하는 조직 혹은 개인을 뜻합니다.

1.6. **업데이트**는 모든 업데이트, 개정, 패치, 강화, 정정, 변경, 복사, 추가 혹은 유지보수 팩 등을 뜻합니다.

2. 사용권 허가

2.1. 권리 소유자는 이로써 소프트웨어를 설치한 귀하의 컴퓨터 보호에 도움을 주기 위하여 일정한 수량의 컴퓨터에서 소프트웨어를 저장, 로드, 설치, 실행 및 디스플레이("사용")할 수 있는 비독점적인 라이센스를 귀하에게 허가합니다. 컴퓨터 보호는 본 계약("라이센스")및 귀하가 승낙한 본 라이센스의 이용약관에 근거한 사용 설명서에서 언급한 위협으로부터 보호함을 의미합니다.

시험 버전 귀하가 이미 소프트웨어의 시험 버전을 받았거나 다운로드 및/혹은 설치하였고 소프트웨어에 대한 평가 라이센스를 허락받았을 경우, 다만 평가 목적으로만 소프트웨어를 사용할 수 있으며 기타 지시가 없는 한 처음 설치일로부터 적용 평가 기간 동안만 사용할 수 있습니다. 기타 목적으로 소프트웨어를 사용하거나 적용 평가 기간을 초과하여 사용하는것은 엄격히 금지되어 있습니다.

다종 환경 소프트웨어, 다종 언어 소프트웨어, 듀얼 미디어 소프트웨어, 다종 카피, 번들 만약 소프트웨어의 다른 버전 혹은 다른 언어판을 사용할 경우, 다종 미디어 소프트웨어를 받았을 경우, 아니면 소프트웨어의 다종 카피를 받았을 경우, 혹은 기타 소프트웨어와 번들된 소프트웨어를 받았을 경우, 모든 버전의 소프트웨어를 설치한 귀하의 컴퓨터의 총 수량은 기타 라이센스 조건이 제공되지 않은 한 권리 소유자가 *제공한* 라이센스 수량과 동일해야 합니다. 구매한 매개 라이센스는 2.2 및 2.3 조항에서 지정한 수량의 컴퓨터에 설치 및 사용할 수 있는 권한을 부여합니다.

2.2. 소프트웨어를 물리적 미디어로써 구매하였을 경우, 소프트웨어 포장에 지정한 수량의 컴퓨터의 보호에 따른 소프트웨어를 사용할 권리를 가지게 됩니다.

2.3. 소프트웨어를 인터넷에서 구매하였을 경우, 소프트웨어의 라이센스 구매시 지정한 수량의 컴퓨터 보호에 소프트웨어를 사용할 권리를 가지게 됩니다.

2.4. 귀하는 다만 백업 목적으로 그리고 합법적으로 소유한 카피가 분실되었거나 파괴 혹은 사용할 수 없을 경우에만 소프트웨어를 복사할 권리를 가집니다. 기타 목적으로 본 백업 카피를 사용해서는 안되며 소프트웨어 사용 권리를 상실, 혹은 라이센스 만기, 혹은 귀하의 주요하게 거주하고 있는 국가의 법률 혹은 현재 소프트웨어를 사용하고 있는 국가의 법률에 의한 임의의 원인으로 라이센스가 강제적으로 종결되었을 경우 백업 카피를 반드시 파기해야 합니다. 귀하는 소프트웨어 사용의 비독점적 라이센스를 권리 소유자가 허락한 라이센스 범위내에서 기타 개인 혹은 실체에게 전임할 수 있습니다. 수납자는 본 계약의 모든 이용약관에 동의하여야 하며 권리 소유자에서 허락받은 라이센스에서 귀하를 완전히 대신하여야 합니다. 권리 소유자로부터 허락받은 소프트웨어의 모든 사용권을 완전히 전임할 경우 귀하는 반드시 백업 카피를 포함한 모든 카피를 파기해야 합니다. 전임한 라이센스의 수납자는 반드시 본 계약의 이용약관에 동의해야 합니다. 만약 본 계약의 모든 이용약관에 동의하지 않으시면 소프트웨어를 설치 및/혹은 사용하지 마시기 바랍니다. 전임한 라이센스의 수납자로서 귀하는 또한 권리 소유자로부터 소프트웨어를 구매한 최초의 최종 사용자가 소유하는 권리외의 추가 권리 혹은 더 많은 권리를 소유하지 않음을 동의합니다.

2.5. 소프트웨어 발효시기부터(소프트웨어 시험 버전은 제외)귀하는 소프트웨어 포장(물리적 미디어로써 소프트웨어를 구매했을 경우)에 지정한 기간 혹은 구매시(소프트웨어를 인터넷에서 구매했을 경우)지정한 기간동안 아래와 같은 서비스 제공을 받을 수 있습니다.

- 권리 소유자가 소프트웨어의 업데이트를 웹사이트 혹은 기타 온라인 서비스를 통해 공개할 경우 인터넷을 통한 소프트웨어의 업데이트를 제공합니다. 본 계약의 이용약관에 적용되며 소프트웨어의 일부로 되는 임의의 업데이트를 받을 수 있습니다.
- 인터넷 및 기술 지원 핫라인을 통한 기술 지원을 받을 수 있습니다.

3. 활성 및 조건

3.1. 귀하가 귀하의 컴퓨터를 변경하거나 혹은 컴퓨터에 설치된 기타 버전의 소프트웨어를 수정할 경우 권리 소유자는 소프트웨어의 활성을 반복할 것을 요구할 수 있습니다. 권리 소유자는 임의의 방법 및 검증 과정을 사용하여 라이센스의 유효성 및/혹은 귀하의 컴퓨터에 설치 및/혹은 사용된 소프트웨어의 카피의 합법성을 검증할 권리를 가집니다.

3.2. 소프트웨어를 물리적 미디어로써 구매했을 경우, 본 계약을 승낙함으로써 포장에 지정한 기간동안 소프트웨어를 사용할 수 있습니다(계약을 승낙한 때부터 시작).

3.3. 본 소프트웨어를 인터넷에서 구매한 경우, 본 계약을 승낙함으로써, 구매시 지정된 기간 동안 사용하실 수 있습니다.

3.4. 귀하는 2.1 조항에서 제공하는 소프트웨어의 시험 버전을 본 계약에 근거한 소프트웨어의 발효시부터 단일 적용 평가기간 동안 무료로 사용할 수 있습니다. 시험 버전은 인터넷을 통한 업데이트 및 기술 지원 그리고 기술 지원 핫라인을 사용할 수 없습니다.

3.5. 귀하의 소프트웨어 사용 라이센스는 3.2 혹은 3.3 조항에서 지정한 바와 같이 시간제한이 있습니다. 남은 시간은 소프트웨어의 그래픽 사용자 인터페이스에서 볼수 있습니다.

3.6. 법적으로 임의의 배상에 대한 편견이 없이 혹은 권리 소유자의 공평성으로, 귀하가 본 계약의 이용약관을 위반하였을 경우, 권리 소유자는 사전 통보없이 언제든지 소프트웨어 사용 라이센스를 중지할 권리를 가지고 있으며 일부 혹은 모든 구매액은 상환하지 않습니다.

3.7. 소프트웨어 사용 및 소프트웨어의 사용결과로 파생된 임의의 리포트 혹은 정보를 사용할 경우, 귀하는 모두 적용되는 국제, 국내, 주, 지역 및 지방의 법률 및 규제를 준수하며, 포함하지만 제한되지 않는 개인 정보 보안, 저작권, 수출 제어 및 음란법을 준수함에 동의합니다.

3.8. 여기에 특별히 언급된 사항을 제외하고 본 계약에 의거하여 귀하에게 부여된 권리 혹은 이에 따라 부여된 의무를 전임 혹은 할당할 수 없습니다.

4. 기술 지원

본 계약의 2.5 조항에서 언급한 기술 지원은 소프트웨어의 최신 업데이트가 완성된후 귀하에 제공됩니다(소프트웨어의 시험 버전은 제외).

5. 정보 수집

5.1. 본 계약의 이용약관에 동의하며, 귀하는 권리 소유자에게 실행 파일 및 검사 합계에 관한 정보를 제공함으로써 귀하의 보안 보호 수준을 개선함에 동의합니다.

5.2. 새로운 위협 및 그 소스에 대한 보안 의식 및 귀하의 보안 보호 수준을 개선하기 위하여, 권리 소유자는 귀하가 동의한 카스퍼스키 보안 네트워크 데이터 수집 정책에 명시된 바와 같이 특별히 이와 같은 정보를 수집할 권리를 갖습니다. 귀하는 설치시 카스퍼스키 보안 네트워크 서비스를 비활성화 할 수 있습니다. 또한 귀하는 소프트웨어 옵션 페이지에서 언제든지 카스퍼스키 보안 네트워크 서비시를 활성화 혹은 비활성화 할 수 있습니다.

귀하는 더 나아가, 권리 소유자는 수집한 임의의 정보를 권리 소유자의 단독 및 독점적 재량에 의하여 추적 및 보안 위험 추세에 관한 공개 리포트에 사용할 수 있음을 인정하고 동의하여야 합니다.

5.3. 소프트웨어는 개인 식별 데이터를 처리하지 않으며 처리 데이터와 임의의 개인 정보를 결합하지 않습니다.

5.4. 권리 소유자에게 전해지는 소프트웨어 정보 수집을 원하지 않으시면 카스퍼스키 보안 네트워크를 활성화 취소 및/혹은 비활성화 해야 합니다.

6. 제한사항

6.1. 적용 법률에 의하여 귀하에게 허락한 권리를 포기하지 않는 한, 귀하는 소프트웨어를 모방, 클로닝, 임대, 대여 리스, 판매, 변경, 디컴파일, 혹은 분해하여서는 안되며 소프트웨어 혹은 그 일부에 근거하여 역어셈블 혹은 파생물을 생성하여서는 안 됩니다. 귀하 및 제 3 자는 또한 소프트웨어 사용자 가독성 소프트웨어를 감소하거나 라이센스한 소프트웨어 혹은 하위 세트를 전임할 수 없습니다. 위 제한이 적용 법률에서 금지됨을 명시하는 것은 예외로 합니다. 소프트웨어의 2 진코드 혹은 소스를 사용하여서는 안 되며 분해하여 사유의 알고리즘 프로그램은 재생성해서는 안됩니다. 본 계약에 명시되지 않은 모든 권리는 권리 소유자 및 혹은 공급자(적용시)가 보유합니다. 소프트웨어의 임의의 비인가 사용은 본 계약 및 허락한 라이센스의 즉시적 및 자동적인 중지를 초래하며 귀하의 형사 및/혹은 민사 공소를 초래할 수 있습니다.

6.2. 본 계약 2.4 조항에서 명시한 외 제 3 자에게 소프트웨어의 사용권을 전임할 수 없습니다.

6.3. 활성 코드 및/혹은 라이센스 키 파일을 제 3 자에게 제공해서는 안되며 제 3 자가 권리 소유자의 기밀 데이터로 간주되는 활성 코드 및/혹은 라이센스 키에 액세스할 수 있게 하여서는 안됩니다. 만일 본 계약 2.4 조항에서 설명한 바와 같이 귀하가 활성 코드 및/혹은 라이센스 키를 제 3 자에게 전임할 경우, 귀하는 활성 코드 및/혹은 라이센스 키의 기밀은 보호하기 위한 적당한 조치를 취해야 합니다.

6.4. 귀하는 제 3 자에게 소프트웨어를 임대,리스 혹은 빌려주어서는 안됩니다.

6.5. 귀하는 소프트웨어를 사용하여 본 사용 설명서에서 설명한 위협들을 탐지, 블록 혹은 처리를 위한 데이터 혹은 소프트웨어를 생성해서는 안됩니다.

6.6. 귀하가 본 계약의 이용약관을 위반하였을 경우 권리 소유자는 상환이 없이 키 파일을 블록하거나 소프트웨어의 사용권을 중지할 권리를 가지고 있습니다.

6.7. 귀하가 시험 버전을 사용할 경우, 본 계약의 4 조항에서 지정한 기술 지원을 받을 권리가 없으며 귀하는 제 3 자에게 라이센스 혹은 소프트웨어 사용권을 전임할 권리도 없습니다.

7. 한정된 보증기간과 면책 성명

7.1. 카스퍼스키 랩은 소프트웨어를 사용자 매뉴얼의 규정과 설명에 의하여 효율적으로 집행할 것을 보증한다. 단 상기 한정된 보증기간은 하기 상황에 적용되지 않는다. (w) 정식 사용자의 컴퓨터에 결함과 관련 침해가 발생할 경우 카스퍼스키 랩은 그 어떤 보수 보증 책임도 부담하지 않음을 명확히 표시한다. (x) 잘못된 사용으로 인한 오작동, 결함, 고장, 남용, 사고, 소홀, 부정확한 설치, 조작 혹은 보수, 도난, 고의적인 파괴, 불가항력, 테러, 전원고장 혹은 서지, 뜻밖의 사고, 변경, 허가를 거치지 않은 수정 혹은 보수로 인한 혹은 카스퍼스키 랩의 합리적인 제어범위를 벗어난 기타 제 3 자 혹은 정식 사용자의 행위 혹은 원인으로 인한 고장, 결함은 보장하지 않는다. (y) 실제 결함이 나타난 이후 사용자가 카스퍼스키 랩에게 바로 알리지 않았을 경우 보증하지 않는다. (z) 정식 사용자의 컴퓨터에 설치한 하드와/ 혹은 소프트웨어 소자로 인하여 겸용이 안 되는 경우 보증하지 않는다.

7.2. 그 어떤 소프트웨어든 오류가 없을 수 없음을 정식 사용자는 승인하고 동의한다. 정식 사용자에게 적합한 빈도와 신뢰에 의거하여 사용 컴퓨터를 백업할 것을 권장한다.

7.3. 사용자 매뉴얼 혹은 본 계약서 조항을 위반한 상황하에 소프트웨어가 정상적으로 운행되더라도 카스퍼스키 랩은 임의의 보증을 제공하지 않는다.

7.4. 본 계약서의 제 2.5 조가 규정한 갱신을 경상적으로 다운로드하지 않았지만 소프트웨어가 여전히 정상적으로 운행되더라도 카스퍼스키 랩은 보증하지 않는다.

7.5. 본 계약서의 제 3.2 혹은 3.3 항이 규정한 유효기간이 만기된 후 혹은 그 어떤 원인이든 소프트웨어 사용허가가 정지된 후 카스퍼스키 랩은 사용자 매뉴얼에 진술된 위험에 대한 보호를 보증하지 않는다.

7.6. 본 소프트웨어는 현황대로 제공되며 소프트웨어의 사용 혹은 성능에 대해 카스퍼스키 랩은 그 어떤 성명도 하지 않으며 그 어떤 보수보증도 제공하지 않는다. 적용 법률이 배제 혹은 제한할 수 없는 그 어떤 보증, 조건, 성명 혹은 조례 외에 제 3 자의 권리, 상업 판매성, 적격 품질, 전체성 혹은 특정 목적의 적용성 등을 침해하는 것을 포함하지만 이에 한하지 않는 그 어떤 사항이든 카스퍼스키 랩 및 그 공급자는 그 어떤 보증, 조건, 성명 혹은 조례(명확한 것 혹은 숨겨진 것, 법령, 보통법률, 관례, 용도 혹은 기타 규정)도 제공하지 않는다. 본 소프트웨어를 선택하여 예상 목적에 도달한 행위와 책임 및 본 소프트웨어를 설치, 사용한 행위와 책임 및 결과에 대하여 정식 사용자는 모든 과실과 위험을 부담한다. 상기 규정을 제한하지 않는 조건하에 카스퍼스키 랩은 그 어떤 성명도 발표하지 않으며 본 소프트웨어가 고장이 없거나 장애 혹은 기타 고장이 발생할 수 없음을 보증하지 않으며 카스퍼스키 랩에게 알렸는지 여부를 막론하고 본 소프트웨어가 정식 사용자의 임의의 요구를 만족함을 보증하지 않는다.

8. 책임 면제와 제한

적용 법률이 허가한 최대 범위내에 그 어떤 상황하에서든지 본 소프트웨어를 사용하거나 사용하지 못한 원인으로 인한, 본 소프트웨어를 통하여 제공되거나 제공되지 못한 지원 혹은 기타 서비스, 정보, 소프트웨어와 관련된 내용으로 인한 , 혹은 본 계약서의 규정에 의한 본 소프트웨어 사용으로 인한, 혹은 계약서를 위반하거나 권리침해 행위 (소홀, 진술 착오, 임의의 엄격한 배상책임 혹은 의무 포함) 로 인한, 혹은 카스퍼스키 랩이나 임의의 공급자가 법정 책임 혹은 보수보증 책임 위반으로 인한 그 어떤 특별한, 부대성, 징벌성, 간접적인 혹은 결과성 손실 (영업 이익 손실 혹은 기밀 정보 소실 혹은 기타 정보의 분실로 인한 손실, 영업중단 손실, 개인정보 분실 손실, 데이터 혹은 프로그램 크래시, 파괴와 분실로 인한 손실, 임의의 법정 의무, 성실 의무 혹은 합리적인 보관 등을 포함한 의무를 이행하지 않음으로 인한 손실, 소홀로 인한 손실, 경제손실과 기타 경제적 측면의 손실 등을 포함하지만 이에 한하지 않음) 에 대해 카스퍼스키 랩 혹은 그 공급자는 정식 사용자가 카스퍼스키 랩 혹은 임의의 공급자에게 이러한 손실의 가능성을 알렸다 해도 그 어떤 책임도 부담하지 않는다.

카스퍼스키 랩과 / 혹은 그 공급자가 책임이 있음을 발견한 상황하에 카스퍼스키 랩과 /혹은 그 공급자의 책임이 본 소프트웨어의 비용에만 한해 있어야 함을 정식 사용자는 동의한다. 그 어떤 상황하에서든지 카스퍼스키 랩과 혹은 그 공급자의 책임은 카스퍼스키 랩과 혹은 그 공급자(적용된 상황하에)에게 지불한 소프트웨어 비용을 초과해서는 안 된다.

본 계약서의 임의의 규정은 인명피해의 클레임을 배제하거나 제한하지 않는다. 그리고 당시 적용된 법률이 본 계약서의 임의의 책임의 면제, 배제 혹은 제한을 배제하거나 제한할 수 없는 상황하에 오직 그 책임의 면제, 배재 혹은 제한만 정식 사용자에게 적용되지만 정식 사용자는 모든 기타 책임의 면제, 배제 혹은 제한의 구속을 계속 받는다.

9. GNU 와 기타 제 3 자 라이센스

본 소프트웨어는 GNU 통용 공공라이센스 (GPL) 에 의하여 사용자 수권라이센스 (혹은 분수권 라이센스) 을 준 일부 소프트웨어 프로그램 혹은 기타 유사 무료 소프트웨어 라이센스를 포함할 가능성이 있다. 이러한 라이센스는 사용자의 어떤 프로그램 혹은 프로그램의 일부를 복사, 수정과 재배분할 것을 허용하며 소스코드("공개소스 소프트웨어")의 사용을 허가한다. 만약 이 라이센스가 임의의 소프트웨어를 실행가능한 바이너리 포맷으로 어떤 사용자에게 배분할 것을 요구할 경우 그 소스코드도 마찬가지로 그 사용자에게 제공되어야 하며 이러할 경우 source@kaspersky.com 에게 청구 혹은 소스코드를 발송해야 한다. 임의의 공개소스 소프트웨어 라이센스가 카스퍼스키 랩으로 하여금 본 계약서가 부여한 권리보다 더욱 넓은 공개소스 소프트웨어 프로그램의 사용, 카피 혹은 수정 권리 제공을 요구할 경우 이 권리는 본 계약서가 규정한 권리와 제한보다 우선권을 가지고 있다.

10. 지적재산권 귀속

10.1 본 소프트웨어 및 본 소프트웨어가 포함한 저작권, 시스템, 관점, 조작방법, 파일과 기타 정보는 카스퍼스키 랩 혹은 그 공급자의 전용 지적재산권과/ 혹은 가치있는 상업 비밀임을 정식 사용자는 동의한다. 또한 카스퍼스키 랩 혹은 그 공급자(구체적인 상황에 의하여 결정함)는 러시아 연방, 유럽연합과 미국의 민법과 형법, 저작권, 상업 비밀, 상표권과 특허권법 및 기타 국가와 국제조약의 보호를 받음을 정식 사용자는 동의한다. 본 계약서는 정식 사용자에게 카스퍼스키 랩 혹은 기타 공급자의 임의의 상표권 혹은 서비스 상표(이하 "상표"라 약칭함)를 포함한 그 어떤 지적재산권도 부여하지 않는다. 정식 사용자는 오직 공인된 상표 규정에 의하여 상표소유자 이름 식별을 포함한 상표표시를 사용하고 본 소프트웨어가 발생한 프린터 제품을 사용할 수 있다. 상기 상표의 임의의 사용도 정식 사용자에게 그 어떤 상표소유권을 부여하지 않는다. 카스퍼스키 랩과/혹은 그 공급자는 본 계약서의 모든 권리, 재산권과 권익을 소유하고 보유한다. 이는 카스퍼스키 랩이 완성했던지 아니면 임의의 제 3 자가 완성했던지, 그리고 본 소프트웨어의 모든 판권,

특허, 상업 비밀권, 상표권과 기타 지적재산권을 막론하고 그 어떤 교정, 개선, 갱신 혹은 기타 소프트웨어의 수정을 포함하지만 이에 한하지 않는다. 정식 사용자는 본 소프트웨어를 소유하고 설치하거나 사용할 수 있으나 정식 사용자에게 본 소프트웨어의 그 어떤 지적재산권을 양도했음을 의미하지 않는다. 본 계약서에서 명확히 규정하지 않았을 경우 정식 사용자는 본 소프트웨어에 대한 그 어떤 권리도 획득할 수 없다. 본 계약서에 의하여 제공된 본 소프트웨어의 카피는 반드시 본 소프트웨어와 동등한 소유권 통지를 포함한다. 본 계약서가 별도로 규정한 경우를 제외하고 본 계약서는 정식 사용자에게 본 소프트웨어에 대한 그 어떤 지적재산권도 부여하지 않는다. 본 계약서가 부여한 라이센스는 정식 사용자에게 본 계약서의 조항과 조건에 의한 한정된 사용 권리만 제공했음을 정식 사용자는 인정한다. 카스퍼스키 랩은 본 계약서가 정식 사용자에게 명확히 부여하지 않은 모든 권리를 보유한다.

10.2 본 소프트웨어의 소스코드, 활성화코드와/혹은 허가 파일은 카스퍼스키 랩이 소유하며 카스퍼스키 랩의 상업 비밀의 일부를 구성함을 정식 사용자는 인정한다. 또한 그 어떤 방식으로도 본 소프트웨어의 소스코드를 수정, 편집, 번역, 역방향 디자인, 해독, 분해 혹은 발견을 시도하지 않을 것을 정식 사용자는 동의한다.

10.3 그 어떤 방식으로도 본 소프트웨어를 수정하거나 변경하지 않을 것을 정식 사용자는 동의한다. 정식 사용자는 본 소프트웨어의 임의의 버전의 임의 판권의 통지 혹은 기타 소유권 통지를 삭제하거나 변경해서는 안 된다.

11. 적용법률; 중재

본 계약서는 법률과 원칙의 충돌에 대해 언급하지 않으며 러시아 연방의 법률의 관할을 받으며 러시아 연방의 법률에 의하여 해석한다. "유엔국제화물판매계약공약"의 관할을 받지 않으며 이 공약의 사용을 명확히 배제한다. 그 어떤 본 계약서 조항의 해석 혹은 사용으로 인한 분쟁 혹은 계약 위반은 직접 협상을 통한 해결을 제외하고 국제상사중재협회의 규정에 의하여 러시아 연방 모스크바에 위치한 러시아연방공상회의 중재에 의하여 해결한다. 중재인이 제출한 그 어떤 판결도 최종적인 것이며 계약 쌍방에게 구속력을 가지고 있으며 이 중재 판결서의 임의의 판결은 임의의 관할권을 구비한 법원에서 집행할 수 있다. 본 계약서 제 11 조의 임의의 규정은 중재 절차 전, 중재 절차기간 혹은 중재 절차 후든지를 막론하고 임의의 일방은 다른 일방이 관할권이 있는 법원에 제출한 공정구제 청구를 막아서는 안 된다.

12. 기소기한

지적재산권의 권리침해소송을 최대 법정 기간내에 제출할 수 있는 것 외에 본 계약서의 거래로 인한 그 어떤 형식의 기소든지 계약 일방이 기소원인이 발생하거나 혹은 발생한 것을 발견한지 1 년이 지난 뒤에 제출해서는 안 된다.

13. 계약서의 완전성; 독립성; 비포기

본 계약서는 정식 사용자와 카스퍼스키 랩 사이에 체결한 완전한 계약서이며 본 소프트웨어 혹은 본 계약서의 세부 사항은 관련된 임의의 기타 구두 계약 혹은 서면의 사전 계약, 건의서, 통신 혹은 건의보다 우선권을 가지고 있다. 정식 사용자는 본 계약서를 이미 읽었고 본 계약서를 이해하며 그 조항의 구속을 받을 것을 동의함을 인정한다. 임의의 관할권이 있는 법원이 본 계약서의 임의의 규정상 전체 혹은 일부가 무효, 무용하며 혹은 임의의 원인으로 인해 이행할 수 없게 되었음을 발견했을 경우 이 규정을 더욱 엄밀하게 해석하여 이를 더욱 합법화하고 효율성있게 하여 이행되도록 해야 하며 이때 전체 계약서는 이로 인해 실효되지 않는다. 본 계약서의 기타 규정은 법률 혹은 평형법이 허용한 최대 범위내에서 계속 효력을 발생하고 최대한 그의 본래의 의도를 견지한다. 정식 사용자와 카스퍼스키 랩의 대리인 사이에 서면동의서를 체결한 경우를 제외하고 본 계약서의 임의의 규정 혹은 조건의 권리 포기는 무효로 되며 본 계약서의 임의의 규정의 위반 권리 포기는 전, 중, 후기 계약 위반의 기권을 제정해서는 안

된다. 카스퍼스키 랩이 본 계약서의 임의의 규정 혹은 권리를 고수하지 못했거나 엄격히 이행하지 못했을 경우 이 규정 혹은 권리에 대한 기권으로 해석해서는 안 된다.

14. 연락 자료

본 계약서에 관한 의문사항이 있거나 그 어떤 이유로 카스퍼스키 랩과의 연락을 원할 경우 저희 고객서비스센터로 연락하십시오.

Kaspersky Lab, 10/1 1st Volokolamsky Proezd
Moscow, 123060
Russian Federation
전화번호: +7-495-797-8700
팩스번호: +7-495-645-7939
이메일: info@kaspersky.com
사이트: www.kaspersky.com

© 1997-2009 Kaspersky Lab ZAO 에서 판권 소유권을 가지고 있다. 본 소프트웨어 및 이와 관련된 임의의 모든 문건은 저작권법과 국제저작권공약 및 기타 지적재산권법과 조약의 보호를 받는다.